Вадим Гребенников
Радиоразведка Европы
Перехват информации

SHOUT
SHARE
IT

Annotation

Любое государство сейчас не может существовать без технической разведки. Радиоразведка появилась вместе с радиосвязью в начале XX века. Книга рассказывает историю рождения и эволюции техники и методов радиоэлектронной разведки и контрразведки спецслужб Великобритании, Германии, Франции, Австрии и Швеции; описывает успехи радиоразведки этих стран по перехвату информации.«Кто владеет информацией, тот владеет миром». (Натан Ротшильд)

- Радиоразведка Европы
  - Предисловие
  - 1. Рождение радиоразведки
  - 2. Радиоразведка Австрии
  - 3. Радиоразведка Швеции
  - 4. Радиоразведка Британии
  - 5. Британская ШКПС
  - 6. Радиоразведка 3-го Рейха
  - 7. Радиоконтрразведка Рейха
  - 8. Радиоигры «Абвера» с «MI6»
  - 9. Радиоразведка Германии
  - 10. Радиоразведка Франции
  - 11. Содружество радиоразведок
  - 12. Радиолокаторы Чехии
  - Эпилог
  - Использованная литература
  - Об авторе

Радиоразведка Европы
Перехват информации
Вадим Гребенников

Предисловие

Книга написана в продолжении развития темы «перехвата» информации и дешифровки переписки противника, которая была изложена в предыдущих книгах по истории криптологии, стеганографии и специальных (секретных) видов связи.

За свою историю разведка накопила большой опыт добывания информации, в том числе с использованием технических средств. Такие задачи инициируют исследования по созданию принципиально новых способов и средств разведки. С этой целью органы разведки ведущих стран имеют мощную научно-производственную базу.

В настоящее время разведку разделяют на агентурную и техническую. Хотя для практики это разделение условное. Условность состоит в том, что добывание информации агентурными методами (агентами) часто осуществляется с использованием технических средств, а техническую разведку ведут люди. Отличия – в преобладании человеческого или технического факторов.

Агентурная разведка является наиболее древним и традиционным видом разведки. Добывание информации производится путем проникновения агента – разведчика к источнику информации на расстояние доступности его органов чувств или используемых им технических средств, копирования информации и передачи ее заказчику.

Применение технической разведки снижает риск задержания агента органами контрразведки или госбезопасности, за счет дистанционного контакта его с источником информации, а также создаёт возможность ведения разведки без нарушения госграницы средствами космической, компьютерной и радиоразведки иностранных государств.

Техническая разведка появилась в процессе технической революции XX века. В основу ее классификации по используемой технике положен физический принцип построения аппаратуры разведки. В соответствии с этим принципом техническая разведка делится на радиоэлектронную, компьютерную, оптическую, оптико-электронную, акустическую, гидроакустическую, химическую, радиационную, сейсмическую и магнитометрическую.

Нас будет интересовать радиоэлектронная разведка «SIGINT» (англ. Signals intelligence) (далее – РЭР), которая делится на радиотехническую, радиолокационную, радиотепловую, радиоразведку и разведку побочных электромагнитных излучений

и наводок (далее – ПЭМИН).

1. Радиоразведка «COMINT» (англ. Communication Intelligence) – направлена на перехват радиограмм и сбор разведданных, основанный на приёме и анализе каналов радиосвязи противника. Радиоразведка посредством перехвата сообщений, исходящих от тех или иных командных инстанций, может получать информацию из самых надежных источников – штабов противника.

Сведения радиоразведки о радиостанциях противника, системах их построения и о содержании передаваемых сообщений позволяют выявлять планы и замыслы противника, состав и расположение его группировок, установить местонахождение их штабов и командных пунктов управления и т. п.

Этот вид разведки обладает следующими особенностями:

– действует без непосредственного контакта с объектами разведки,

– охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот,

– функционирует непрерывно в разное время года и суток и при любой погоде,

– обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации)

– добывает большое количество информации различного характера и содержания,

– получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени,

– малоуязвима и во многих случаях недосягаема для противника,

– действует скрытно, поскольку противник, как правило, не в состоянии установить факт разведки.

2. Радиотехническая разведка «ELINT» (англ. Electronic intelligence) – вид радиоэлектронной разведки по обнаружению и распознаванию радиолокационных станций (далее – РЛС), радионавигационных систем и систем связи, использует методы радиоприема, пеленгования и анализа радиосигнала. Средства радиотехнической разведки позволяют:

– установить несущую частоту передающих радиосредств;

– определить координаты источников излучения;

– измерить параметры импульсного сигнала (частоту повторения, длительность и другие параметры);

– установить вид модуляции сигнала (амплитудная, частотная, фазовая, импульсная);

– определить структуру боковых лепестков излучения радиоволн;

– измерить поляризацию радиоволн;

– установить скорость сканирования антенн и метод обзора пространства РЛС;

– проанализировать и записать информацию.

3. Радиолокационная разведка – предназначена для получения радиолокационного изображения (обстановки). В радиолокаторе формируется зондирующий узкий, сканирующий по горизонтали и вертикали луч электромагнитной волны, которым облучается пространство с объектом наблюдения. Отраженный от поверхности объекта радиосигнал принимается радиолокатором и модулирует электронный луч электронно-лучевой трубки его индикатора, который, перемещаясь синхронно с зондирующим лучом, «рисует» на экране изображение объекта.

4. Радиотепловая разведка добывает информацию о признаках объектов, проявляющихся через их собственные электромагнитные излучения в радиодиапазоне.

5. Разведка ПЭМИН использует ту же радиоаппаратуру и методы, что и радиоразведка. Только эта аппаратура предназначена для улавливания очень слабых сигналов, то есть она более чувствительная.

Различают наземную, морскую, воздушную и космическую РЭР. По своему содержанию информация, добываемая этим видом разведки, делится на оперативную и техническую.

Оперативная информация включает сведения, которые необходимы для решения оперативных задач военного командования. К ним относятся:

– открытая или зашифрованная смысловая информация, передаваемая противоборствующей стороной по различным каналам радиосвязи,

– тактико-технические данные и особенности разведываемых активных радиоэлектронных средств и систем (далее – РЭС), состовляющие их «электронный почерк»,

– типы РЭС: радиосвязи, радиолокации, радионавигации, различные телеметрические системы передачи данных,

– количество обнаруживаемых РЭС противника,

– местоположение и территориальная плотность размещения источников излучения электромагнитной энергии противника.

Изучая технические характеристики и особенности РЭС противника, можно определить область их применения и принадлежность. Сопоставляя эти данные с уже известными, полученными разведкой по другим каналам, можно сделать вывод о назначении разведываемых технически средств.

Зная это и определяя типы и количество РЭС противника, можно установить дислокацию войсковых частей, военных баз, аэродромов и других объектов.

Для анализа и обработки добываемой информации очень важное значение имеют точная фиксация времени начала и конца работы излучающих РЭС и правильное определение их местоположения. Эти данные позволяют установить степень активности противника в определенной территориальной зоне.

Техническая информация содержит сведения о новых системах оружия и управления радиоэлектронными устройствами и об их электрических характеристиках, используемыми разведываемой страной впервые. Целью добывания технической информации является своевременная разработка аппаратуры и методов РЭР новых систем оружия и средств управления противника.

Для получения такой информации средствами РЭР ведется систематическая разведка новых, ранее неизвестных источников радиопередач, отличающихся диапазоном частот, видами модуляции и манипуляции, параметрами импульсного сигнала, диаграммой направленности антенны и другими характеристиками.

Особенности РЭР заключаются в следующем:

– действует без непосредственного контакта с объектами разведки;

– охватывает большие расстояния и пространства, пределы которых определяются особенностями распространения радиоволн разных частот;

– функционирует непрерывно в разное время года и суток и при любой погоде;

– обеспечивает получение достоверной информации, поскольку она исходит непосредственно от противника (за исключением случаев радиодезинформации);

– добывает большое количество информации различного характера и содержания;

– получает информацию в кратчайшие сроки и чаще всего в реальном масштабе времени;

– малоуязвима и во многих случаях недосягаема для противника;

– действует скрытно (противник, как правило, не в состоянии установить факт разведки).

Также нас будет интересовать и компьютерная разведка – целенаправленная деятельность по добыванию с помощью средств вычислительной техники (далее – СВТ) и программного обеспечения (далее – ПО) разведывательной информации,

обрабатываемой в СВТ и информационно-вычислительных сетях (далее – ИВС), а так же информации об особенностях их построения и функционирования.

Целью компьютерной разведки является добывание сведений о предмете, конечных результатах, формах и способах деятельности субъектов, являющихся пользователями компьютерной сети и используемом аппаратном и программном обеспечении, протоколах управления и информационного взаимодействия и используемых средствах и методах защиты информации.

Важнейшая роль в достижении информационного господства отводится виртуальной разведке – разведке, ведущейся в информационных потоках, которые в гигантских количествах производятся всеми государственными и частными организациями, а также отдельными лицами. Компьютерную разведку ещё называют виртуальной разведкой.

Виртуальная разведка ведется в компьютерных сетях, средствах массовой информации (далее – СМИ) и непериодических изданиях, в том числе открытых и так называемых «серых», не имеющих грифа секретности, но не предназначенных для массового распространения.

Виртуальная разведка представляет собой целый комплекс взаимосвязанных действий оперативно-технического характера. Важнейшей технической компонентой виртуальной разведки является компьютерная разведка. Она делится на добывающую и обрабатывающую. Задача добывающей разведки состоит в получении данных, а обрабатывающей – в преобразовании данных в информацию и приведение ее в форму, удобную для пользователя.

Добывающая разведка бывает предварительной и непосредственной. Задача предварительной разведки – получение сведений о самой автоматизированной системе (далее – АС) противника, обрабатывающей защищаемую информацию. Цель предварительной разведки – подобрать данные, необходимые для последующего проникновения в АС противника.

Цели предварительной разведки достигаются путем добывания открытых и закрытых сведений. К открытым сведениям можно отнести данные о характере и режиме работы АС объекта разведки, квалификации его персонала, составе и структуре самой АС, используемом ПО, протоколах управления и взаимодействия, средствах и методах защиты информации, используемых в АС.

Для получения этих сведений нет необходимости прибегать

к приемам оперативной работы (подкупу персонала, краже документации и т. п.). Эти сведения, как правило, не являются закрытыми и могут быть получены при перехвате сетевого трафика интересующей АС или попытке установить сетевое соединение непосредственно с самой АС, когда по характеру получаемого отклика можно сделать соответствующие выводы.

Установление первичного контакта с АС противника, как правило, еще не дает доступа к интересующей информации. Для этого необходимо получить дополнительные сведения закрытого характера. К таким сведениям относятся пароли, коды доступа, информация о принятых в АС правилах разграничения доступа и сетевые адреса СВТ объекта.

Для получения подобных сведений существуют разнообразные шпионские программные средства. К ним относятся, например, программы перехвата всех команд, вводимых в АС. Другим средством являются программы считывания первых 128 бит каждого файла, в которых нередко помещается служебная информация о самом файле и об АС.

Существуют также специальные программы подбора паролей. Успеху подобных программ способствуют многочисленные ошибки в современном ПО, что объясняется его сложностью и относительной новизной. Помимо ключей, интерес представляет перехват кусков зашифрованного текста с заранее известным содержанием.

Это позволяет выделить из шифрограммы секретный ключ, который используется для дальнейшего криптоанализа всего текста. Сведения, собранные об АС противника подобным образом, открывают путь к добыванию информации, интересующей заказчика, т. е. к ведению непосредственной разведки.

На стадии непосредственной разведки, как и на всех остальных, добываются не только закрытые, но также «серые» и открытые сведения. Роль открытых сведений в достижении общей ситуационной осведомленности о противнике достаточно велика.

Важнейшим достоинством перехвата открытых сведений при ведении компьютерной разведки является то, что эти сведения могут быть получены без нарушения принятых в АС правил разграничения доступа к информации. Сбором и анализом открытых сведений в сетях официально занимается множество организаций, которые за определенную плату выполняют заказы на поиск той или иной информации.

Добывание закрытых сведений всегда связано с несанкционированным доступом (далее – НСД) к информации

противника и имеет своим следствием утечку информации. Получение закрытых сведений осуществляется как в самой АС объекта, так и в ИВС, внешних по отношению к АС.

Во внешних сетях перехватываются те сообщения, которые объект разведки пересылает внешним адресатам, либо в случае виртуальной сети, те сообщения, которые циркулируют между отдельными сегментами АС. Программное проникновение в АС объекта с целью ведения разведки может осуществляться несколькими способами. Отдельную группу таких способов составляет проникновение через несетевые периферийные устройства (клавиатуру, дисководы и т. п.).

Наиболее многочисленная и динамично развивающаяся группа способов программного проникновения в АС противника – это проникновение из внешних сетей. Можно выделить два основных пути такого проникновения:

– проникновение с использованием паролей и идентификаторов, найденных в результате предварительной разведки;

– поиск уязвимостей и ошибок (к называемых «черных ходов») в аппаратном и программном обеспечении, используемом в АС.

При применении указанных способов проникновения, недостаточно лишь добраться до винчестера противника и «скачать» с него данные. Необходимо восстановить удаленные файлы противника и тщательно разобраться в полученном объеме сведений. Эту функцию выполняет обрабатывающая разведка.

Обработке подвергаются данные, полученные как в отдельном СВТ, так и в ИВС, при этом сеть представляет дополнительные возможности по обработке. Посредством анализа трафика можно контролировать гигантские потоки сведений, производить отбор, накопление и обработку не всех данных подряд, а только тех, которые представляют интерес для заказчика.

Для ведения экспресс-анализа в сети созданы специальные программы, так называемые «ноуботы» (англ. Knowbot – Knowledge Robot – робот знаний), которые способны перемещаться в ИВС от между СВТ и при этом размножаться, создавая копии. «Ноубот» вводится в компьютерную систему и, обнаружив интересующую его информацию, оставляет в этом месте свою копию, которая собирает информацию и в определенное время передает ее.

С целью исключения обнаружения в «ноуботе» могут быть предусмотрены функции самоперемещения и самоуничтожения. С помощью средств компьютерной разведки можно не только

анализировать конкретные данные, циркулирующие во всей сети, безотносительно к их источнику, но и отслеживать деятельность конкретных организаций и отдельных лиц.

Особо следует подчеркнуть, что обработке подвергаются не только закрытые, но и открытые сведения. Соответствующий анализ открытых источников позволяет синтезировать информацию закрытого характера. По оценке специалистов изучение 10000 открытых документов позволяет при некоторых условиях получить 1 документ высшей степени секретности.

В связи с высокой степенью угрозы безопасности информации, обрабатываемой в ИВС, все большее количество пользователей сети применяют для защиты своей информации шифрование. По этой причине одной из задач обрабатывающей компьютерной разведки является применение криптоаналитического ПО.

Кроме вооруженных сил компьютерной и радиоразведкой занимаются государственные спецслужбы и правоохранительные органы, добывая при этом, в основном, оперативную информацию путем перехвата шпионских радиограмм и электронной переписки подозреваемых лиц. А теперь обо всем поподробней…

1. Рождение радиоразведки

С момента рождения радио в 1895 году и по мере его внедрения как средства связи и управления оно стало использоваться во всех странах в интересах государственной и военной разведки.

В 1902 году в Великобритании был опубликован рассказ Редьярда Киплинга под названием «Беспроволочный телеграф», в котором описывались опыты по перехвату радиосигналов. Процесс радиоперехвата в рассказе уподоблялся спиритическому сеансу – те же «обрывки посланий, долетающие невесть откуда, отдельные слова, а в целом – ничего не разберешь».

«Беспроволочный телеграф» был интересен тем, что в нем впервые открыто обсуждались вопросы, связанные с радиоразведкой. В рассказе было правильно показано, что в начале 1900-х годов для того, чтобы использовать эфир в качестве источника разведывательной информации, не требовалось ничего, кроме оборудования, которое позволяло слушать чужие радиопереговоры.

Однако по мере того, как такое оборудование получало все большее распространение, лица, общавшиеся между собой посредством радио, стали прибегать к помощи шифров, чтобы сделать содержание своих сообщений недоступным для других. Поэтому помимо перехвата эфирных сигналов для ведения радиоразведки вскоре понадобилось взламывать шифры, которые применялись для засекречивания передаваемых сообщений.

Уже в начале XX века ведущие мировые страны вели слежку за работой радиостанций своих противников и прослушивание их радиопередач. Известно, что с 1902 года британский флот, а с 1903 года американский флот в ходе учений опробовали перехват вражеских радиопереговоров.

Однако интенсивно разведка радиотехническими средствами стала использоваться воюющими странами и их союзниками с началом русско-японской войны в 1904 году. Так, британские корабли систематически перехватывали радиопередачи русских боевых кораблей, находившихся в Средиземном море (в том числе осуществлявших переход на Дальний Восток).

В 1914 году в Европе началась Первая Мировая война. 1 августа Германия объявила войну России, а 3 августа – Франции, а также нейтральной Бельгии, отказавшейся пропустить немецкие войска через свою территорию. 4 августа Великобритания со своими доминионами объявила войну Германии, а 6 августа Австро-Венгрия – России.

В августе 1914 года войну Германии объявила Япония, в октябре – на стороне блока Германии и Австро-Венгрии в войну вступила Турция, а в октябре 1915 года – Болгария. Италия, изначально занимавшая позицию нейтралитета, в мае 1915 года под дипломатическим давлением Великобритании объявила войну Австро-Венгрии, а 28 августа 1916 года – Германии.

С первых месяцев войны перехват радиосообщений противника позволил получать ценные сведения о его намерениях, о расположении и перегруппировке неприятельских войск. Этому способствовало нарушение элементарных правил радиообмена со стороны штабов армий и фронтов, передававших по радио секретные приказы и распоряжения открыто или с применением несложных шифров.

Воюющие стороны, убедившиеся в утечке информации через радиосвязь, вскоре стали применять более сложные шифры и строже регламентировать свои радиопередачи. Однако нарушения радиодисциплины продолжались.

Наблюдая и изучая характерные особенности действующих радиосвязей противника, их интенсивность, позывные, стабильность, рабочие частоты, тон сигнала работающих радиостанций, «почерк» радистов, продолжительность и время передач старых и вновь появившихся радиостанций, незначительные признаки нарушения радиообмена и т. п., радиоразведка была в состоянии вскрывать оперативные замыслы командования, следить за перемещением войск и получать другие важные сведения о противнике.

Если в начале войны для радиоразведки использовались приемные устройства связных радиостанций, то в последующие годы воюющие стороны стали применять специальные радиоприемники и создавать первые подразделения службы радиоразведки.

Радиопеленгаторы как средство войсковой и морской радиоразведки впервые появились в действующих армиях Российской империи, Великобритании, Германии, Австро-Венгрии в 1915—16 годах.

Радиопеленгаторная аппаратура внесла новое содержание в радиоразведку и принципиально расширила ее возможности. С помощью радиопеленгаторов стали определять местонахождение вражеских радиостанций и тем самым устанавливать районы нахождения штабов, частей и соединений, время начала и направление их перемещения.

Британская радиоразведка, имея хорошо организованную службу радиоперехвата и криптоанализа, систематически дешифровывала немецкие секретные радиограммы, передаваемые

не только штабами частей и соединений армии, но и правительством, генеральным штабом, посольствами и другими ведомствами.

Особенно успешно действовала военно-морская разведка Великобритании. Ее центром была «комната 40» британского адмиралтейства, где высококвалифицированные криптоаналитики расшифровывали перехваченные радиограммы.

Британская радиоразведка сыграла важную роль в морской войне своего флота с немецкими подводными лодками (далее – ПЛ), блокирующими Великобританию со всех сторон. Криптограммы, посылаемые германским морским командованием по радио своим ПЛ, перехватывались британцами и дешифровывались.

Они достали с морского дна несколько кодовых книг Военно-морского флота (далее – ВМФ) Германии, находящихся в затопленной немецкой ПЛ, и пользовались ими при дешифровке радиограмм.

В истории британской радиоразведки важное место занимает Ютландское сражение. В конце мая 1916 года британцы перехватили переданный немцами по радио секретный приказ о выходе немецкого ВМФ в море для нанесения внезапного удара по британскому ВМФ. Британцы дешифровали содержание приказа и стали скрытно готовиться к отражению атаки.

В результате британцы навязали немцам неожиданное для них сражение в 90 милях к западу от северной оконечности Ютландского полуострова, в котором немцы понесли тяжелые потери.

Важный след оставила британская радиоразведка и в нашумевшем в свое время заявлении Президента США Вудро Вильсона, сделанном 1 марта 1917 года, накануне вступления США в Первую Мировую войну на стороне союзников.

В нем было заявлено, что министр иностранных дел Германии Артур Циммерман предложил мексиканскому правительству присоединиться к Германии, чтобы объявить США войну.

Естественно возник вопрос, каким образом немецкий совершенно секретный документ попал на стол американского президента. Оказалось, что британская радиоразведка перехватила шифртелеграмму Циммермана, переданную по радио, дешифровала ее и немедленно передала американскому послу в Лондоне.

Немецкая радиоразведка в Первой Мировой войне также выдавала весьма ценные сведения о противнике военному командованию. Известно, что в отдельные периоды войны немцы

дешифровывали в сутки до 300 секретных радиограмм своих противников.

Начальник разведывательного управления Верховного командования Вооруженных сил Германии в период 1913—19 годов Вальтер Николаи в своих мемуарах поведал, что достоверным источником сведений являлись перехваченные русские радиопередачи.

В связи с этим коротко расскажу о событиях, которые произошли в Восточной Пруссии в августе 1914 года. Штаб второй русской армии генерала Александра Самсонова, не имея связи со своими наступающими корпусами, передал им по радио открытым текстом ряд секретных приказов, которые были перехвачены немецкой радиоразведкой.

В результате немцы получили ясную картину действий противника на ближайшие дни. Немецкое командование грамотно использовало полученные разведданные, и после активных действий немцев русская армия была разгромлена.

Австрийская радиоразведка действовала весьма успешно с самого начала Первой Мировой войны и информировала свое верховное командование и германское командование о всех перехваченных приказах и донесениях, которые передавались по радиотелеграфу.

Книга начальника разведывательного бюро Генерального штаба (далее – ГШ) Австрии генерала Макса Ронге содержит большой фактический материал о деятельности австро-венгерской радиоразведки за весь период Первой Мировой войны.

Она содержит многочисленные примеры работы радиоразведки, данные которой позволяли оценить оперативную обстановку до начала проведения той или иной операции и послужили основанием для планирования и проведения боевых действий.

Так, например, во время Галицийской операции, в начале сентября 1914 года, когда между 1-й и 2-й австрийскими армиями образовался разрыв, австрийская радиоразведка получила сведения о том, что в направлении прорыва двигаются крупные соединения русских. В результате австрийское командование приняло решение об отходе всех австрийских армий за реку Сан.

Болгария первый опыт ведения радиоразведки в армии и на флоте получила в ходе Балканской войны 1912—13 годов. На флоте в этих целях накануне и в ходе Первой мировой войны использовались стационарная радиостанция «Франга» (около н. п. Голяма Франга, ныне – Каменар), корабельная радиостанция на борту крейсера «Надежда», четыре береговые радиостанции (2 стационарные в н. п. Галата и Карантината, 2 подвижные).

Болгарский офицер Г. Д. Сколуфанов вспоминает, что для того, чтобы избежать помех от радиостанций вооруженных сил Болгарии турки прибегали к хитрости. Они начинали радиопередачу на волне 600 м, а когда понимали наше вмешательство, переходили на волну 1200 м. Факт того, что турецкие радиотелеграфисты меняли частоты радиосвязи, защищая свою информацию, показывает, что они опасались перехвата своих радиограмм.

Италия до Первой мировой войны проявляла к радиоразведке и криптоанализу незначительный интерес. Тем не менее, к началу войны там появилось несколько весьма одаренных радиоразведчиков. Лучшим среди них был Луиджи Сакко, 32-летний лейтенант инженерных войск, служивший на радиостанции Верховного командования. Первых результатов в радиоразведывательной деятельности он добился в ходе итало-турецкого конфликта 1911 года.

Сакко, который возглавлял итальянскую службу перехвата, удалось самостоятельно дешифровать перехваченные радиограммы. Восстановленные им участки открытого текста оказались настолько ценными, что его назначили главой дешифровального отдела при Верховном командовании. Отдел в целях конспирации назывался Шифровальным подразделением и первоначально состоял всего из 3-х человек. Однако к концу войны в нем служили уже несколько десятков сотрудников.

Итальянские радиоразведчики и криптоаналитики добились полного чтения австро-венгерских криптограмм во время битвы при Гориции в августе 1917 года. Растущий опыт итальянских разведчиков помогал им решать все более сложные задачи, например, вскрыть австрийский дипломатический код.

Готовой к войне в эфире оказалась и радиоразведка Франции. Заслуга в этом принадлежала созданным еще в довоенное время дешифровальным органам, более мощным и лучше организованным, чем в других странах. Криптбюро, созданное Ф. Картье в военном министерстве, было обеспечено мобилизованным персоналом. В первые дни интенсивность радиосвязи противника была низкая, но когда немецкие войска в начале августа 1914 года пересекли границу Франции, выйдя за пределы своих телеграфных линий, количество их радиопередач резко увеличилось.

Сначала французские станции радиоперехвата находились лишь в крупных крепостях и в 3-х специальных пунктах перехвата, а 6 радиопеленгаторных станций находились вдоль линии фронта. Позднее к ним добавились еще 2 пункта перехвата в Париже – один на Эйфелевой башне, другой – на станции

парижского метро «Трокадеро».

Радиоразведчикам военного министерства приходилось оказывать помощь МИД в чтении дипломатической переписки на линии связи Берлин – Мадрид. Подопечные Картье читали также и военно-морскую шифрпереписку немцев, поскольку французский флот не имел в своем штате криптоаналитиков.

В частности, ими был вскрыт шифр немецких ПЛ. Французы обнаружили, что каждую полночь подпольная радиостанция в г. Науне посылала немецким ПЛ в Средиземном море время выхода и маршруты французских судов, отплывавших из Марселя. Радиоразведчики перехватывали сообщения немецких шпионов, а криптоаналитикам требовалось не более часа, чтобы их дешифровать. В результате вносились изменения в расписание рейсов и маршруты перехода судов. Многие из раскрытых кодов Германии французы отправляли англичанам.

Уже к 1915 году Криптбюро превратилось в первое в мире полноценное государственное ведомство радиоразведки. Оно имело в штате несколько десятков человек, из которых 9 были криптоаналитики. Главе Криптбюро подчинялась также шифровальная служба ГШ. По мнению Ф. Картье его подчиненные перехватили за время Первой мировой войны более 100 миллионов слов.

Радиоразведку русского флота в водах Балтийского моря, перехват и дешифрование дипломатической переписки Германии в ходе Первой мировой войны, несмотря на проводимую политику нейтралитета, осуществляли и подразделения радиоразведки Швеции.

Все это свидетельствует, что радиоразведка во время Первой Мировой войны развивалась и как постоянно действующая структура, как и один из основных видов разведки вооруженных сил Российской империи, Австро-Венгрии, Великобритании, Германии, Италии, США, Франции, Болгарии, Швеции и Японии.

Процессы строительства радиоразведки как структуры и совершенствования ее деятельности как вида разведки протекали в этих государствах со своими особенностями и различными результатами. Тем не менее, общими чертами этого периода являлись специализация сил и средств радиоразведки, консолидация усилий различных ведомств в области добывания информации и криптоанализа, организация взаимодействия с союзниками.

2. Радиоразведка Австрии

Должность начальника разведгруппы Разведывательного Бюро ГШ «Эвиденцбюро» Вооруженных сил Австро-Венгрии перед Первой Мировой войной занимал Максимилиан Ронге. Он в 1911—12 годах добился включения в состав группы нескольких офицеров, специалистов в области шифрования и дешифрования.

Он в своей книге «Разведка и контрразведка», изданной в 1939 году, привел интересные сведения о работе австрийской радиоразведки на фронтах Первой Мировой войны. Официально австрийская служба радиоразведки и дешифровки появилась в структуре Разведывательного Бюро только к апрелю 1917 года. В дальнейшем появились дешифровальные службы и группы на фронтах.

Особенно выдающимся специалистом в сфере дешифровки был капитан Герман Покорный, начальник русского отделения дешифровальной службы. Соответственно, можно констатировать, что австрийское командование вступило в войну с высококвалифицированными кадрами специалистов-радиоразведчиков, что в дальнейшем принесло свои плоды.

Уже в начале войны при австрийских армейских командованиях находились рации, передававшие перехваченные депеши в разведывательный отдел (фронтовой центр дешифрования). Эти рации занимались исключительно наблюдением за рациями соединений русской армии.

Очень ценным источником информации оказалась русская радиотелеграфная переписка. Русские пользовались своими радиотелеграфом так легкомысленно, как будто не предполагали о наличии радиоприемников, которые можно настроить на соответствующую волну.

К тому же поначалу русские радисты нередко вставляли открытый текст в шифрованный. Вскоре одновременное использование открытых и шифрованных текстов в сообщениях было запрещено, но было уже слишком поздно, и оно сыграло свою негативную роль.

10 сентября 1914 года во время сражения под Львовом создалось критическое положение. Русским не удалось разбить наше северное крыло; южное же крыло, во главе с начальником генштаба фон Конрадом, двигалось к Львову. Радиоразведка получила секретные сведения о том, что русские войска двигаются по направлению к пустому пространству, образовавшемуся возле 1-й армии. Так как резервов для обеспечения тыла фронта у австрийцев не было, то было принято

решение об отступлении.

14 сентября австрийцы перехватили распоряжение Ставки русских войск о необходимости полностью зашифровывать все военные сообщения, передаваемые по радио. Однако переход на шифрованные радиопередачи не изменил положения дел. Имея большой опыт по перехвату русского радиообмена, на основании его анализа австрийцам удалось дешифровать русский шифр. Дешифровка первой русской радиограммы заняла около 4-х суток, после чего австрийцы продолжали вести эффективную радиоразведку.

При отступлении австрийских войск в Галиции со взятием русскими войсками Перемышля австрийская радиоразведка перехватила радиограмму, посланную командиром русского кавалерийского корпуса генералом Александром Новиковым, которая представляла большую разведывательную ценность. Эта радиограмма была быстро дешифрована и представлена немецкому командованию.

Примерно в это же время русские впервые сменили шифр. Сами строки остались без изменений, но изменился порядок выбора строк для шифрования. Новый шифр был вскрыт Покорным 19 сентября в течение нескольких минут: все трудности отпали, когда одна из русских радиостанций передала зашифрованную новым шифром телеграмму, переданную еще до смены шифра.

Она не имела нового шифра и сообщила об этом по радио передающей станции, с которой последовала повторная передача этой же телеграммы, но зашифрованной старым шифром, что позволило дешифровальщикам легко вскрыть новый шифр.

Кроме того, новая шифрсистема не представляла серьезных трудностей для криптоаналитиков, поскольку в шифртексте сохранялась структура часто используемых в открытом тексте слов, таких как «атака», «дивизия», которые полностью шифровались одной строкой таблицы.

Первую важную шифртелеграмму Покорный прочитал 25 сентября. Это было длинное донесение Новикова о результатах разведки с примечанием в конце: «Я принял решение не форсировать Вислу». Шифртелеграмма была отправлена в 08—40 утра, а в 16—00 офицер связи довел до сведения немецкого штаба ее содержание. Знание принятого Новиковым решения обеспечило успех действий австро-германских войск в начальной стадии битвы на реке Висла.

Другой пример: из телеграммы полковника русской кавалерийской дивизии князя Ингалищева немцы узнали о готовившемся наступлении на крепость Перемышль.

Предупрежденный об этом комендант крепости успешно отражал атаки, пока наступление австрийских войск не вынудило нападавших в середине октября снять осаду крепости. Во время этого наступления группа Покорного читала ежедневно до 30 русских шифртелеграмм.

4 октября 1914 года австрийская радиоразведка перехватила радиограмму русского полковника князя Енгалычева из 10-й кавалерийской дивизии в Саноке. Из нее стало известно о предполагавшейся атаке на юго-восточных фортов Перемышля, о чем было немедленно оповещено по радио командование крепости. Капитан Покорный продолжал неустанно работать над дешифровкой радиоперехвата, и ему удавалось прочитать до 30 телеграмм в день.

11 октября немецкая армия под командованием Августа фон Макензена вклинилась в русскую оборону. В 14—10 следующего дня начальник штаба одной из русских армий, по которым был нанесен удар, передал по радио длинную шифровку. Кроме даты запланированной атаки в шифровке указывалась наиболее уязвимая зона в боевом порядке этой армии – стык между ее войсками и армией соседа.

На следующий день дешифрованная и переведенная радиограмма уже лежала в штабе немецких войск Восточного фронта, а ее содержание было немедленно передано Макензену. В 19—30, имея перед собой карту со схемой расположения русских, он отдал приказ о переходе подчиненных ему войск в наступление по всему фронту с нанесением главного удара в стык двух армий.

К этому времени русские ежедневно меняли порядок использования шифралфавитов, но по-прежнему оставляли без изменений сами шифралфавиты. В результате австрийские дешифровщики без перебоев читали их шифрпереписку. Поток информации, добываемой с помощью радиоперехвата, не сокращался. Немцы уже настолько привыкли к этому, что 19 октября Макензен не отдавал приказов до тех пор, пока не были получены сведения от дешифровщиков.

Следующий день стал черным для дешифровальной группы. В перехваченной шифртелеграмме 4-й русской армии содержалось предупреждение о том, что немцы имеют ключи к русскому шифру. Русские сумели захватить ключи к немецкому шифру и предположили, что аналогично мог поступить и противник. В действие был введен новый шифр, причем на этот раз – с заменой всех элементов шифрсистемы.

На Восточный фронт опустился занавес молчания. Лишенные глаз и ушей, армия Макензена к 21 октября оказались в «мешке».

Русские предвкушали победу и уже заказали поезда для вывоза военнопленных. Но на следующий же день группа Покорного вскрыла новый шифр, и в немецкий штаб вновь пошел поток ценной информации. Из него немцам стало известно слабое место в кольце русских войск. К 25 октября 1914 года кольцо окружения было успешно прорвано.

Ежедневно австрийская служба радиоперехвата наблюдала за передвижением русских войск. 7 ноября она успела предупредить немецкую армию о готовившейся на нее атаке, благодаря чему серьезно подготовленное нападение успеха не имело. 3-й кавказский корпус 4-й русской армии и два соседних корпуса столкнулись друг с другом, и при этом возникло замешательство.

Оба командующих армиями яростно «бомбили» друг друга телеграммами, что доставило австрийцам большое удовольствие. Не меньшую радость доставил им приказ командования 5-й русской армии, требовавший от генерала Орановского посылать все указания по радио, так как восстановление разрушенных линий связи на театре военных действий требовало слишком много времени и сил. Этот приказ давал нам возможность беспрепятственно отслеживать большую часть мероприятий на Восточном фронте.

Служба радиоперехвата представляла бесценную информацию австро-германскому военному командованию. Можно было определить намерения русского командования и обеспечить учет вооруженных сил противника. В результате уже к концу октября была установлена точная дислокация частей, до дивизий включительно.

13 ноября был перехвачен и дешифрован приказ о переходе на следующий день во всеобщее наступление русской армии вглубь Германии, после чего сразу попал на стол канцелярии Главнокомандующего Восточным фронтом. Из этого приказа было, видно, что русские не имели никакого представления об угрозе их северному флангу и о силах перешедшей 12 ноября в наступление 9-й германской армии, которая расценивалась ими в один корпус.

20 ноября какой-то офицер связи 4-й русской армии передал по радио другому офицеру, что действующий шифр известен противнику. Затем австрийцы узнали из другой радиограммы, что русские раскрыли немецкий шифр и поэтому узнали о том, что их шифр тоже известен противнику.

В результате русские заменили шифр, после чего австрийские и немецкие посты радиоперехвата скурпулезно собирали новые шифровки. К 22 ноября общими усилиями удалось раскрыть

и этот новый шифр. Криптоаналитикам помогло, что русские, привыкшие к шаблону, придерживались привычной им шифровальной системы.

К сожалению, первым переданным сообщением было известие о прорыве немецкого окружения под Лодзью. Русские сообщения позволяли точно следить за действиями немецких частей.

В начале декабря австрийцы перехватили следующую русскую радиограмму: «Шифровальный ключ, не исключая посланного в ноябре, известен противнику». Тем не менее, русские продолжали пользоваться старым шифром. То ли у них было недостаточно других средств связи, то ли не было в запасе нового шифра, или же они считали достаточной частую смену позывных радиостанций, что во всяком случае удлиняло дешифровальную работу.

6 декабря 1914 года генерал Новиков сообщил, что он неожиданно получил приказ прикрыть отход 19-го русского корпуса. Это было первым признаком того, что русская армия начала свое отступление, по крайней мере, на северном фланге.

14 декабря новый русский шифр лишил нас источника сведений. Раскрытие нового шифра было сложным делом. Однако совместная кропотливая работа майора Глумака, капитана Покорного и обер-лейтенантов Земанека и Маркезетти дала возможность его раскрытия в течение нескольких дней.

К весне 1915 года в русских войсках полностью отказались от старой системы шифров и стали применять простой шифр Цезаря. Большое количество таблиц, использовавшихся в условиях ведения активных боевых действий, и ежедневная смена ключей ставили непосильную задачу перед связистами. В этих условиях вскрытие очередного русского шифра для дешифровальной службы не составило почти никакого труда.

Чтение русских криптограмм позволило принимать время от времени такие меры, которые были единственно правильным тактическим решением в данной ситуации. Российский ГШ был озадачен прозорливостью противника. Однажды немцы оставили занимаемые ими позиции за 2 дня до начала большого наступления русских войск. Одним из объяснений точного соответствия решений немецкого командования создавшейся обстановке русские считали использование им аэрофотосъемки и агентурной разведки.

Но постепенно крепло убеждение, что противник читает русскую шифрпереписку. Когда немецкое весеннее наступление 1915 года достигло апогея, русские опять сменили шифр. Но эта смена доставила больше хлопот им самим, так как почти все шифровки, переданные по радио в первые 2 дня после смены

шифров из-за допущенных ошибок так и не были прочитаны адресатами.

В марте 1916 года австрийская радиоразведка получила стройную организацию, при этом для каждой станции радиоперехвата был определен определенный участок Восточного фронта. Во время русского наступления австрийцы оказали большую помощь немецким войскам, перехватив соответствующие приказы русского командования.

Главным руководителем австрийской радиоразведки был назначен капитан Болдескул, занявший место майора Покорного. Болдескул получил в подчинение 6 станций или групп радиоперехвата, которые находились в Барановичах, Ковеле, Берестечке, Бродах, Бржезанах и Коломые.

Австрийцы ежедневно дешифровывали до 70 радиограмм с оперативными приказами, сводками, о перемещениях командиров и т. п. Новые правила радиопередачи и новый шифр, объявленные 16 июня, вызывали недовольство русских штабов вследствие их сложности.

Ввиду этого ряд штабов продолжал пользоваться старым шифром и правилами, что в огромной степени облегчало раскрытие нового шифра. Штаб гвардейской группы, включенной в состав 8-й армии, передал в незашифрованном виде ключ нового шифра.

За этим последовал взрыв возмущения в штабе 8-й русской армии и введение штабом Юго-Западного фронта нового шифра. При этом было передано сообщение с помощью старого шифра, что при подготовке криптограммы вторичной перешифровки не требуется.

23 мая 1915 года Италия объявила войну Австро-Венгрии, поэтому австрийская радиоразведка работала и на итальянском фронте. Сначала она встречала затруднения из-за неспособности дешифровывать перехваченные радиограммы. Однако со временем австрийцы хорошо изучили принципы шифрования итальянских радиограмм и стали их читать.

После того, как итальянская полевая радиослужба начала передавать не только сведения, касающиеся непосредственно службы связи, но и оперативные распоряжения, австрийцы ежедневно стали дешифрировать до 50, а в отдельные сутки до 70 криптограмм.

Тем не менее, итальянцы уже в начале 1916 года располагали большим количеством станций радиоперехвата. Так, в течение одного полугодия они смогли подслушать около 5200 радиоразговоров, что причинило австрийцам большой вред.

К этой работе ими было привлечено большое количество

дезертиров и перебежчиков, знавших немецкий язык. В октябре 1916 года к ним перебежал начальник одной станции радиоперехвата, детально их ознакомивший с нашей организацией прослушки.

Прослушка, прежде всего, давала данные тактического порядка, а, кроме того, давала высшему командованию ценные сведения и обеспечивала проверку данных других видов разведки. Это было важно, поскольку противник умышленно направлял к нам перебежчиков для дезинформации. Они нередко обладали такой ловкостью и смелостью, что им удавалось вернуться обратно к своим.

Свыше 30 австрийских радиостанций осуществляли непрерывное наблюдение за таким же количеством итальянских станций. Каждая перехваченная радиограмма дешифровывалась австрийцами в кратчайший срок.

22 февраля итальянцы ввели новую весьма остроумную систему позывных для радиостанций. Над ней австрийцам пришлось долго ломать голову, но все же к 7 марта она была раскрыта и сообщена персоналу радиостанций. 30 марта 1916 года итальянское главное командование запретило дальнейшее применение шифра «Cifrario rosso» в радиообмене в связи с подтвердившимся подозрениями о частичной компрометации этого шифра. На самом же деле он был раскрыт целиком и полностью.

Известный интерес для австрийцев представляла радиосвязь между итальянской главной квартирой в Удине и отдельным корпусом в Валлоне, хотя ею сравнительно мало пользовались благодаря исправности подводного кабеля между Корфу и Италией. Тем не менее, преодолев первоначальные затруднения, наши мощные радиостанции в Сараево, Петервардейне, Мостаре, Каттаро и Скутари добыли ряд важных сведений, передача которых продолжалась с помощью шифра «Cifrario rosso».

Кроме того, радиостанции в Скутари было передано все, относившееся к шифрам итальянского флота. В кратчайший срок она использовала эти материалы и оказала поддержку морской станции из Пола. В самой Албании итальянцы пользовались шифром «Менгарини», ключ которого был куплен австрийской разведкой еще до войны. Это сослужило хорошую службу радиостанции в Скутари и немецкому дешифровальному отделу в Ускюбе.

Болгария вступила в Первую мировую войну 14 октября 1915 года на стороне Германии и Австро-Венгрии, объявив войну Сербии. 27 августа 1916 года Румыния объявила войну Австро-

Венгрии, поэтому австрийская радиоразведка работала и на румынском фронте.

Вначале дешифровка румынских радиограмм была сопряжена с большими трудностями, но вскоре эта работа полностью себя оправдала, поскольку румыны, как и русские, передавали по радио оперативные приказы. Благодаря этому, австрийцы получили полную картину обстановки на фронте.

Так, австрийской радиоразведкой был перехвачен детальный оперативный приказ о контрнаступлении 14 сентября 1916 года добруджской армии, усиленной войсками из Трансильвании. Уже 16 сентября разведывательное бюро смогло передать в штаб 1-й армии в Колошвар (Клаузенбург) первые дешифрованные радиограммы, относившиеся к румынским войскам в Трансильвании.

Для радиоразведки наступили лучшие времена. В Софии был организован радиоразведывательный центр во главе с капитаном Янши, помощником которого был назначен капитан Маросан, имевший уже большие заслуги в деле дешифровки.

В этот центр поступали перехваченные сообщения не только от болгарских радиостанций перехвата, но и с радиостанций на румынском фронте. После дешифровки они передавались главному командованию и в армейскую группу Макензена, объединившую 1-ю и 9-ю армии.

Хоть румыны строго и запрещали незашифрованную радиопередачу, но с шифрованными радиограммами обращались настолько неосторожно, что австрийцам пришлось выделить дополнительного дешифровальщика штабу 1-й армии для разгрузки радиостанции перехвата в Софии.

В начале войны с Румынией русские прилагали все усилия к тому, чтобы своим наступлением содействовать ожидавшемуся успеху. Благодаря радиоперехвату группы капитана Болдескула, получившей затем название «Австро-Норд» (группа капитана Янши стала называться «Австро-Зюйд»), наступательные намерения русских всегда своевременно выявлялись.

24 сентября для дешифровальщиков стало «черным» днем. Из-за потери 6-м русским кавалерийским корпусом шифров военного министерства для радиосвязи, радиограмма добруджской армии запрещала передачу оперативных приказов по радио.

Одновременно румынские сухопутные радиостанции прекратили передачу. Продолжала действовать лишь радиосвязь между морским ведомством и дунайской флотилией и связь главной квартиры с добруджской армией. 6 ноября радиогруппа дунайской русской армии перестала пользоваться «шифром

службы связи №14» из-за его вероятной компрометации.

17 декабря радиопередача на русском юго-западном и на русско-румынском фронтах снова полностью прекратилась, поскольку радиостанция 1-й терской казачьей дивизии была захвачена противником. Радиосвязь стала «оживать» лишь с 21 декабря, причем стал применяться шифр, введенный 14 декабря.

Очевидно, русские шифровальщики не хотели «головной боли». В то же время австрийцам попались французские зашифрованные радиограммы, появившиеся в связи с прибытием для реорганизации румынской армии французской военной миссии во главе с генералом Анри Бертело.

В 1917 году в радиоразведке была создана организация «Австро-Вест». Радиопеленгаторные станции, существовавшие до сих пор лишь в виде опыта, получили определенную организацию и должны были путем ежедневных измерений проверять дислокацию итальянских радиостанций.

На юго-западном фронте наряду с немногими отдельными станциями, были созданы следующие группы по 4 станции в каждой:

– «Пенкала Боцен» – в составе 4-х таких групп (Финоккио, Обербоцен, Тоблах, Крейцберг;

– «Пенкала Виллах» – в составе 8 отдельных станций;

– «Пенкала Адельсберг» – из 2-х групп (Адельсберг, Буйе).

Генерал Бороевич приказал особо хорошо обеспечить «Пенкала», поскольку итальянцы имели на фронте Изонцо большое число радиостанций – не менее 80, из них около 30 мощных. Каждой группе или отдельной станции была отведена определенная зона прослушки с таким расчетом, чтобы за каждой радиостанцией противника наблюдали 2—3 станции.

Дешифровку радиограмм осуществляла «Пенкала» юго-западного фронта, только в случае смены позывных или шифра криптограммы отправлялись в Баден. Радиостанции в Албании принимали помимо итальянских и сербских радиограмм, зашифрованных самыми простыми шифрами, еще французские. Из 3-х французских шифров немцы раскрыли 2, австрийцы – 1.

24 октября 1917 года в разгар наступления австро-германских войск на итальянском театре военных действий для «Пенкала» выдался удачный день. Одна за другой итальянские радиостанции подавали очень приятный сигнал: «свертываемся».

На некоторое время «Пенкала» были обречены на бездействие, поскольку шифр «Cifrario rosso» был заменен новым шифром ГШ, раскрытие которого потребовало кропотливой работы. Тем временем, 21 ноября были перехвачены

радиограммы, указавшие на прибытие 46-й французской пехотной дивизии.

В ночь на 23 ноября 1917 года по приказу начальника итальянской радиосвязи все радиостанции сообщили центральной станции о своем местонахождении и расположении отдельно стоящих штабов. Благодаря этому, австрийцы быстро установили дислокацию всех итальянских соединений, включая и находившиеся поблизости в резерве.

Группам «Пенкала» пришлось заняться раскрытием нового шифра итальянских стационарных радиостанций, которые были включены в полевую сеть связи. Кроме того, итальянский офицер связи при салоникской армии стал пользоваться новым шифром.

Тем же шифром начальник итальянской военной миссии в Румынии генерал Ромен телеграфировал своему главному командованию о положении румынских и русских войск. Делал он это как раз в тот момент, когда русские радиостанции замолчали, за что австрийцы были ему очень признательны.

«Пенкала Баден», кроме того, должна была обрабатывать радиопереписку Италии со своими колониями, которая стала осенью весьма оживленной. Из нее стало известно о прекращении призыва в войска населения Северной Африки и других колоний. Это было особенно важно, поскольку после полученных потерь у итальянцев осталось мало сил для сопротивления.

Прибытие англичан и французов в Италию поставило перед австрийскими мастерами радиоразведки и дешифровки совершенно новые задачи. Трудности были связаны с тем, что первоначально войска находились на отдыхе, поэтому радиопередач было мало. Тем не менее, австрийцами еще на Балканах был накоплен большой материал по французскому радиотелеграфу. Первая французская радиограмма была перехвачена 23 декабря 1917 года.

Осознание важности и успешности работы австрийской радиоразведки содержал доклад итальянской следственной комиссии о сражении при Карфрейте:

«Достаточно указать на высокий уровень развития у противника радио подслушивания, дополненный изумительными достижениями по дешифровке шифров. Благодаря этому, противник выяснил наши пути отхода, определяя наши радиостанции и расшифровывая их радиограммы. Документы, захваченные после окончания войны, показывают, что противником были раскрыты почти все наши шифры, включая наиболее сложные и самые секретные».

Характерно, что как только итальянцы получили от дезертира немецкий радиоприемник, они тотчас же завели такие

радиоприемники у себя. Показательно также, что ни один из австро-германских штабов не хотел отказаться от своих «Пенкала», когда нужно было уменьшить их число при сокращении фронта.

В результате принятого главным командованем решения маршал Конрад получил «Пенкала Боцен», генерал Бороевич – «Пенкала Сен-Вито», а эрцгерцог Евгений – «Пенкала Удине». Число радиогрупп было сокращено до 6, поэтому кроме указанных «Пенкала» остались только группы Финоккио и Штадлен.

Наступившая в результате революций 1917 года дезорганизация русской армии оказала отрицательное воздействие и на ее службу радиосвязи. Пропорционально снижению дисциплины в войсках росла болтливость радистов. В начале года только в течение одного дня австрийская дешифровальная служба прочла более 300 русских шифртелеграмм, из чего следовало, что служба обеспечения безопасности связи в России быстро разваливалась.

С начала 1918 года станции телефонной прослушки, освободившиеся на русском фронте, позволили увеличить их число на юго-западном фронте до 82. Это было особенно важно в связи с тем, что условия местности и редкие боевые столкновения сильно уменьшили количество пленных и перебежчиков.

Вместе с тем налаженная итальянцами проводная связь ослабила эффективность работы австрийской радиоразведки. Однако благодаря офицеру связи при итальянском 20-м корпусе, который начал в марте по несколько раз в день передавать зашифрованные радиограммы, австрийцы оказались в курсе всех боевых действий.

Были результаты и у «слухача» на Кастеллачио – лейтенанта Кареты, и у «слухачей» на Пазубио – лейтенантов Торзиелло и Адамо. В апреле австро-германские войска совершенно прекратили пользование радиосвязью, так как была замечена активность итальянцев в деле радиоперехвата. Поэтому по радио разрешалось передавать лишь шифровки с дезинформацией.

В то же время итальянские войска начали передавать по радио зашифрованные обзоры боевой обстановки. Особенно этим страдал командующий 1-й армией генерал Пекори-Джиральди. Так, например, в течение 1—4 мая путем радиоперехвата была установлена дислокация всех армейских и 20 корпусных штабов из 25, 37 дивизий из 57 и всех кавалерийских дивизий.

Однако вскоре итальянцы стали пользоваться радиосвязью

только в самых экстренных случаях. Все же, благодаря приказу начальника итальянской радиослужбы полковника Кардона об обязательных донесениях радиостанций, австрийская радиоразведка перед началом наступления давала почти такие же богатые результаты, как и раньше на русском фронте. Полковник Кардона даже не догадывался, что сам предупредил противника о предстоящей смене шифра 6 июня.

В последний год войны в «Эвиденцбюро» во главе с Максом Ронге, включая внутреннюю разведку, работало около 300 сотрудников, 50 должностных лиц, 400 агентов полиции, 600 солдат и 600 информаторов.

В 1918 году экономический кризис, сложная обстановка на фронте и распад соседней Российской империи послужили причиной распада Австро-Венгрии. В результате 28 октября была провозглашена Чехословакия, а 29 октября – Государство словенцев, хорватов и сербов.

31 октября в Будапеште произошло вооружённое восстание, и император Австро-Венгрии Карл I потерял контроль над страной. 1 ноября была провозглашена Западно-Украинская народная республика, а 6 ноября – Польша. В тот же день Карл I отрёкся от престола, и Австро-Венгрия прекратила своё существование.

Несмотря ни на что, австрийская радиоразведка продолжала свою кропотливую работу. Даже 1 ноября было обработано 65 шифрованных итальянских радиограмм и были правильно установлены группировки и направление движения итальянских армий. Лишь 3 ноября 1918 года, после заключения перемирия, австро-венгерская разведывательная служба вместе со своей радиоразведкой прекратила свою деятельность.

3. Радиоразведка Швеции

Начиная с лета 1928 года, радиоразведка в Швеции велась только ВМС и то нерегулярно. Ведение радиоперехвата было возложено на боевой корабль «Sverige», однако с лета 1929 года к решению задач радиоразведки были дополнительно привлечены несколько кораблей из состава сил охраны военно-морских баз, а с октября того же года радиоразведка стала вестись и с береговых узлов связи.

В начале 1930-х годов командование ВМС Швеции предприняло дополнительные меры, направленные на повышение роли радиоразведки. По его инициативе в 1930—31 годы были организованы курсы по подготовке специалистов в области криптографии и криптоанализа. На курсы, которые действовали вплоть до 1935 года, принимались действующие офицеры, а также призванные на военную службу студенты и офицеры запаса. Несколько позднее на курсах стали обучаться криптоанализу гражданские специалисты университета Упсала. Помимо изучения теоретических основ криптологии слушатели курсов получали хорошую практическую подготовку по дешифрованию реальных материалов радиоперехвата. Начиная с весны 31-го, корабли ВМС Швеции с выходом на дозорную службу вблизи побережья страны стали осуществлять регулярный перехват радиопередач кораблей и узлов связи иностранных государств. С целью повышения профессиональной подготовки были организованы постоянные тренировки радиооператоров на корабле «Drottning Victoria».

В 1936 году правительство Швеции, учитывая сложную международную обстановку, приняло решение об очередном реформировании вооруженных сил страны. Планами военной реформы предусматривалось изменение организационной структуры и увеличение численности частей военно-воздушных сил, введение должности верховного главнокомандующего и образование Объединенного штаба, на который возлагались задачи по управлению всеми видами вооруженных сил страны. В рамках проводимой реформы произошли изменения и в организации военной разведки. С 1 июля 1937 года в составе Министерства обороны Швеции начали работу 3 новых отдела – разведывательный, радиоразведки и криптологии.

Формально ответственность за организацию радиоразведки была возложена на управление связи штаба вооруженных сил, однако на практике задачи радиоразведки по-прежнему решались кораблями и подразделениями ВМС – единственного вида

вооруженных сил Швеции, располагавшего подготовленными радиооператорами и специалистами радиоразведки.

В состав отдела криптологии вошли 4 секции, три из которых отвечали за обеспечение криптографической безопасности систем связи соответственно сухопутных войск, ВВС и ВМС, а четвертая секция должна была заниматься вопросами криптоанализа шифров и кодов иностранных государств. Все работы отдела предписывалось осуществлять в обстановке глубокой секретности, для чего под его нужды было выделено небольшое, но отдельное здание, которое среди сотрудников стало именоваться «Серым домом». Накануне Второй мировой войны численность отдела возросла, в связи с чем ему были предоставлены помещения на одном из этажей Военной академии. Вскоре и этих помещений оказалось недостаточно, поэтому при очередном увеличении численности сотрудников секция криптоанализа была переведена из академии в отдельное здание.

Утром 30 ноября 1939 года войска Ленинградского военного округа под командованием генерала К. Мерецкова пересекли советско-финляндскую границу и стали продвигаться вглубь Финляндии, что фактически означало начало войны. В тот же день Президент Финляндии Кюёсти Каллио заявил, что «Финляндия объявляет состояние войны».

Именно в годы этой войны, вошедшей в историю как советско-финская кампания или Зимняя война, началось сотрудничество Швеции и Финляндии в области радиоразведки и криптоанализа. Нарядус отправкой добровольцев и поставками вооружения Швеция передавала своему соседу разведывательные данные, полученные путем радиоперехвата и чтения шифр переписки сухопутных частей Красной Армии. Шведским криптоаналитикам удавалось также дешифровывать радиотелеграфные сообщения советских ВВС. Многие из них содержали приказы о нанесении бомбовых ударов по столице Финляндии. Очень часто эти криптограммы дешифровывались еще до момента вылета советских бомбардировщиков с аэродромов, расположенных в Латвии и Эстонии всего в 20 минутах полета от Хельсинки. Благодаря этому, финские власти имели достаточный запас времени, чтобы заблаговременно предупредить население города о готовившихся воздушных налетах.

Зимняя война продолжалась 105 дней и завершилась подписанием 12 марта 1940 года мирного договора в Москве. Однако важные события во взаимодействии разведслужб Швеции и Финляндии были еще впереди.

9 апреля 1940 года немецко-фашистские войска вторглись в Данию и Норвегию. В ходе проведения Германией морской десантной операции норвежскими средствами береговой обороны были уничтожены 7 немецких транспортных судов, на борту которых находились войска и вооружение, в том числе и различная техника связи.

Испытывая трудности в организации управления войсками, находившимися на территории Норвегии, Германия обратилась к правительству нейтральной Швеции с запросом об использовании ее линий телефонной и телеграфной связи, проходивших по западному побережью страны.

Получив согласие, командование немецких войск уже с 18 апреля приступило к их использованию. Помимо этого Германия продолжала передачу дипломатических сообщений по отдельной линии, связывавшей немецкое посольство в Стокгольме с Берлином, а начиная с середины июня 1941 года приступила также к использованию новой линии связи Стокгольм – Гельсингфорс. Всего в годы войны в интересах Германии использовались 4 линии телеграфной связи из Осло в направлении Нарвика, Стокгольма, Копенгагена, Берлина и Тронхейма.

Испытывая несмотря на нейтралитет тревогу за безопасность своей страны, военно-политическое руководство Швеции решило не упускать уникальный шанс оказаться в курсе планов немецкого военного командования. В результате уже в конце апреля 1940 года шведская радиоразведка подключилась к доступным ей телеграфным линиям связи и стала осуществлять перехват передаваемых по ним открытых и зашифрованных сообщений.

Одновременно с началом перехвата немецких сообщений шведскими криптоаналитиками была предпринята попытка проникнуть в тайны функционирования немецкой буквопечатающей аппаратуры связи. Результат не заставил ждать себя очень долго – первое представление о принципах шифрования, использовавшихся в машине Т-52А/В, было получено секцией криптоанализа уже 25 мая 1940 года. Полученные 27 мая дополнительные материалы перехвата и результаты их анализа подтвердили правильность первоначально сделанных предположений, что позволило уже через две недели сформулировать основные принципы устройства и работы немецкой шифровальной машины.

Основная заслуга в раскрытии шифра принадлежала руководителю группы шведских криптоаналитиков профессору Арне Берлингу. Будущий математик родился 5 февраля 1905 года. После школы поступилв университет Упсала, а по его

окончании остался в нем на преподавательской работе. В 1934 году он защитил диссертацию, а в 37-ом стал профессором университета. Научные интересы Берлинга были достаточно широки – отдельные вопросы функционального анализа, теории чисел, теории интегрального исчисления. Перед началом Второй мировой войны Берлинг совместно с группой профессоров, специалистов в области славянских языков и литературы, математики и астрономии, принимал участие в дешифровании закрытого радиообмена кораблей Северного и Балтийского флотов, а также частей Красной Армии. После окончания войны Берлинг в течение 10 лет продолжал трудиться в университете Упсала, после чегоперебрался в США и длительное время работал в Институте перспективных исследований в Принсетоне, штат Нью-Джерси.

Вскоре после того, как Берлингу удалось проникнуть в тайны построения и функционирования немецкой шифрмашины, к работам криптоаналитической секции были подключены несколько технических специалистов во главе с Виго Бергструмом. Им было поручено создание дешифровальных машин в соответствии со схемами, подготовленными группой криптоаналитиков под руководством Арне Берлинга. Уже несколько первых таких машин в значительной мере облегчилии ускорили работу шведских специалистов по взлому зашифрованных немецких телеграмм. Позднее изготовление достаточно большой партии таких машин было налажено на заводе точной механики Эриксона.

Дешифрование немецких телеграмм продолжалось достаточно долго – с июня 1940 по май 1943. Шведские криптоаналитики успешно справлялись с возложенной на них задачей, несмотря на неоднократную смену ключевых процедур и появление на контролируемых линиях телеграфной связи более совершенных моделей немецких шифровальных машин. Перехват сообщений осуществлялся на буквопечатающие аппараты, расположенные в том же здании, где размещалась криптоаналитическая секция. Первоначально использовались аппараты американского производства. Поскольку их число было невелико, а доставка новых аппаратов в военное время из США была затруднена, секцией некоторое время использовались аппараты, предоставленные в ее распоряжение шведской администрацией телесвязи. В результате пострадали шведские телеграфисты, вынужденные на отдельных линиях связи вновь вернуться к старому способу передачи сообщений – с использованием кода Морзе. Вскоре криптоаналитики получили необходимое количество немецких буквопечатающих аппаратов

фирмы Siemens.

Поступающие с аппаратов телеграфные ленты наклеивались на специальные бланки и передавались специалисту, отвечавшему за вскрытие шифрключей. Как правило, он ожидал, когда в его распоряжении окажется несколько телеграмм, зашифрованных с использованием одного и того же ключа, а происходило это достаточно часто по причине систематического нарушения установленных правил немецкими операторами.

В связи с плохим качеством и большой протяженностью шведских линий связи прием сообщений сопровождался большим количеством ошибок и нарушений синхронизации, в результате чего принятые телеграммы становились нечитаемыми. Это вынуждало операторов передавать одно и то же сообщение по несколько раз. В отдельных случаях число повторов составляло от 20 до 40. Поскольку процедура установки нового ключа сообщения представляла собой довольно утомительное занятие, операторы шли на сознательное нарушение инструкций и передавали повторное сообщение с прежней установкой ключа. В результате у криптоаналитика оказывалось несколько одинаковых сообщений (отличающихся друг от друга за счет ошибок), зашифрованных одним и тем же ключом. Это и позволяло вначале определить ключ сообщения, а затем прочитать само сообщение с использованием дешифровальной машины.

Несомненно, что работе криптоаналитика предшествовала весьма трудоемкая деятельность его коллег по выявлению суточного ключа и схем коммутации ключевых колес с электромеханическими реле шифрмашины.

Поток сообщений, передаваемых по контролируемым линиям связи, непрерывно возрастал – если в 1940 году было передано только 7100 телеграмм, то в 1941 их число возросло уже до 41400, а в 1942 – до 120800 (из них 101000 шифрованных). В связи с увеличивавшимся объемом работ по дешифрованию телеграмм росла и численность секции криптоанализа – в 1941 году в ней трудилось уже около 500 человек.

До осени 1940 года поток перехватываемых сообщений был невелик. При этом информация, содержавшаяся в дешифрованных немецких телеграммах, не вызывала какого-либо беспокойства со стороны военно-политического руководства Швеции – ни командование вермахта, ни сам Гитлер не проявляли к Швеции значительного интереса. Это позволило криптоаналитической секции наладить свою работу и отработать порядок взаимодействия сподразделениями штаба вооруженных сил и министерством иностранных дел.

В соответствии с заведенным порядком все дешифрованные сообщения, в которых содержались важные сведения стратегического характера, доставлялись из криптоотдела лично полковнику Карлосу Адлеркройцу – начальнику разведывательного отдела штаба вооруженных сил Швеции. После ознакомления с документами Адлеркройц прибывал с ними на доклад к главнокомандующему вооруженными силами генералу Олофу Торнеллу и начальнику штаба вооруженных сил генералу Акселю Раппе. После этого дешифрованные телеграммы поступали к сотрудникам разведотдела для учета и систематизации содержавшихся в них сведений. Телеграммы, содержащие менее важные сведения, поступали в разведотдел сразу же после их дешифрования.

По мере изучения содержавшейся в них информации все дешифрованные телеграммы сжигались. Исключение составляли только особо ценные с военно-стратегической точки зрения. Круг лиц, которым было разрешено ознакомление с материалами дешифрования, был ограничен небольшим количеством сотрудников штаба. При этом ознакомление осуществлялось на выборочной основе – информация доводилась только до тех лиц, кому это было необходимов силу исполнения своих служебных обязанностей.

В министерство иностранных дел и секретную службу Швеции материалы дешифрования отсылались только по личному указанию начальника разведотдела. При этом в МИД материалы направлялись в весьма ограниченном количестве, поскольку Адлеркройц считал, что в этом ведомстве слишком мало внимания уделяется сохранению государственной тайны и опасался утечки информации.

Однако, благодаря хорошим отношениям МИД с руководством криптоотдела, сложившимся еще при прежнем министре Ричарде Сандлере, сотрудники дипломатического ведомства получали интересующую их информацию «из первых рук». В свою очередь МИД также оказывал специалистам криптоотдела весьма важные услуги, информируя их о важнейших событиях, сведения о которых могли содержаться в зашифрованной переписке немецких дипломатов. Это в значительной степени помогало шведским криптоаналитикам в их работе по дешифрованию перехваченных телеграмм. Адлеркройц был крайне недоволен тем, что часть информации попадает в МИД, минуя его, и в течение длительного времени предпринимал безуспешные попытки подчинить себе отдел криптологии.

Начиная с зимы 1941 года военно-политическая обстановка

вблизи Швеции становилась все напряженнее. Уже в феврале руководство третьего рейха зондировало возможность переброски немецких войск и вооружения из Норвегии в Финляндию через территорию Швеции. Однако теперь военное командование и МИД страны имели возможность принимать решения исходя из более объективной оценки происходящих событий. Этому способствовало систематическое получение разведывательных данных относительно состава, дислокации и планов использования немецко-фашистских войск на территории соседней Норвегии. Достоверность получаемых сведений сомнений ни у кого не вызывала.

21 апреля сотрудниками криптоаналитической секции была дешифрована важная телеграмма. В ней содержался длинный перечень немецких воинских частей, которые должны были в ближайшее время начать «передвижение в северном направлении». Вместе с тем, из телеграммы следовало, что немецкое командование не планирует каких-либо действий против Швеции. Сведения подтверждались и дополнялись данными, полученными разведотделом от шведских приграничных воинских частей, таможни, полиции, а также показаниями беженцев, прибывших на территорию страны из Норвегии. Перехваченные и дешифрованные сообщения, которыми обменивался МИД Германии со своим посольством в Стокгольме, также не давали поводов для беспокойства со стороны Швеции.

4 июня было перехвачено сообщение о планируемой переброске крупной группировки немецких войск в северную часть Финляндии с территории Германии и Норвегии в срок до 15 числа того же месяца. Спустя неделю были дешифрованы еще 3 телеграммы, еще раз подтвердившие сделанный шведской разведкой еще в конце апреля вывод о том, что Финляндия примет участие в войне с Советским Союзом на стороне Германии. 16 июня вступила в действие линия связи Берлин-Гельсингфорс, проходящая через Стокгольм. В тот же день шведской разведке из дешифрованной телеграммы стало известно о некоторой активизации немецких войск в финской Лапландии.

Все эти факты свидетельствовали о неминуемом приближении войны. Тем не менее, руководство Швеции, будучи уверенным в том, что предстоящая война ее не коснется, и желая сохранить в тайне такой исключительно ценный источник информации как дешифрованные немецкие телеграммы, решило никаких мобилизационных мероприятий в стране не проводить.

С началом боевых действий немецко-фашистских войск

против Советского Союза стал стремительно нарастать поток сообщений, адресованных командованию группировок немецких войск в Осло и Рованиеми. Возросло и количество зашифрованных дипломатических депеш, передаваемых на линии связи Стокгольм-Берлин. Информация, получаемая военно-политическим руководством Швеции в 1941—1942 годах в результате дешифрования немецких телеграмм, становилась все более обширной и подробной. Вместе с тем, она носила в определенном смысле локальный характер, что определялось теми задачами, которые возлагались руководством третьего рейха как на немецкое посольство в Стокгольме, так и на командование немецких войск в Норвегии и Финляндии.

Успехи, достигнутые специалистами радиоразведки и криптоанализа, явились одной из причин того, что1 июля 1942 года на базе объединения отделов криптологии и радиоразведки в составе Министерства обороны Швеции была образована самостоятельное Радиоуправление национальной обороны «FRA» (шв. Forsvarets Radioanstalt).

Примерно в это же время в штабе вооруженных сил Швеции стало известно об утечке информации, относящейся к дешифрованию немецкой переписки.

Еще в сентябре 1941-го по указанию заместителя начальника штаба вооруженных сил Швеции генерала Сэмюэля Окерхельма была подготовлена специальная инструкция, определявшая порядок обращения с материалами дешифрования. Основная цель инструкции состояла в исключении раскрытия столь важного источника разведывательной информации, каким являлось дешифрование закрытых сообщений иностранных государств. В соответствии с инструкцией все работы по обработке и передаче материалов дешифрования должны были осуществляться с соблюдением мер секретности и безопасности. Строго запрещалось какое-либо упоминание об этих материалах в разговорах, при ведении телефонных переговоров и в письменных документах. Определялся порядок уничтожения дешифрованных телеграмм. Тем не менее, несмотря на все предпринятые в штабе меры безопасности, утечка произошла.

В этой связи начальник иностранного отдела штаба в своем письме к военному атташе Швеции в Гельсингфорсе сообщал: «Произошло чрезвычайное происшествие. Немецкое командование было проинформировано финнами о том, что нам удалось вскрыть машинный шифр, используемый в аппаратуре Т-52, и в течение продолжительного времени читать шифрованные телеграммы. В результате произведена полная смена ключей, задействованы новые каналы связи…».

Достоверными сведениями о том, как произошла утечка, шведы не располагали. По одной из версий, возможной причиной утечки явилось излишне доверительное отношение ряда высокопоставленных лиц Швеции к военному атташе Финляндии в Стокгольме полковнику Стевэну, в результате чего финской разведке и стало известно о дешифровании шведами немецкой переписки.

Стевэн находился под наблюдением немецкой службы безопасности и подозревался в том, что он собирает и передает шведской стороне важные сведения, которые, спустя некоторое время, становятся известными США и Великобритании. Не исключено, что когда немцы стали оказывать давление на своего союзника с целью отстранения Стевэна от должности военного атташе, финны, в порядке компенсации ущерба, причиненного немецкой стороне, поделились с ней информацией об успехах шведской дешифровальной службы. Последствия всей этой туманной истории для шведской стороны оказались катастрофическими – немецкое командование, начиная с 17 июня, начало предпринимать беспрецедентные меры по обеспечению безопасности засекреченной связи.

Одна из первых мер – появление на контролируемых шведами линиях связи с 21 июля 1942 года новой модификации шифрмашины Т-52С. Как выяснилось позднее, в машине стал использоваться более сложный метод формирования ключевой последовательности. Поэтому первоначальные попытки вскрыть шифр закончились для шведских криптоаналитиков полным провалом. Только спустя 2 месяца им удалось разобраться в особенностях функционирования новой машины и приступить к дешифрованию телеграмм.

Другая мера предосторожности, предпринятая немецким командованием, заключалась в прекращении передачи наиболее важных сообщений по линиям связи, проходящим через территорию Швеции. В результате шведская разведка лишилась сведений о составе, дислокации и деятельности немецко-фашистских войск на территории Норвегии и Финляндии. Положение ухудшилось в еще большей степени в октябре 1942 года, когда вся телеграфная переписка Германии с Осло и Рованиеми стала осуществляться только через территорию Дании и Норвегии, либо по специально проложенным по дну Балтийского моря кабельным линиям. Таким образом, под контролем шведской радиоразведки остался только дипломатический канал связи немецкого посольства в Стокгольме. Однако и здесь шведской стороне пришлось столкнуться с определенными трудностями.

Начиная с октября немцы в целях улучшения криптографической защиты сообщений стали использовать специальный режим «Wahlwerter», предусматривающий включение в начальную часть телеграммы какой-либо фразы, состоящей из случайно выбранных слов. При введении такого режима немецкие криптографы исходили из хорошо известного факта, заключающегося в том, что многие телеграммы по своей структуре являются однотипными. Знание структуры сообщения в определенной мере облегчало работу криптоаналитика по дешифрованию сообщения. Теперь его работа должна была стать намного сложнее. Включение в телеграмму случайной фразы должно было приводить к нарушению ее структуры, поскольку адресная группа и заголовок должны были смещаться на случайное число знаков.

Однако недопонимание сути затеи или немецкая педантичность привели к тому, что многие операторы стали использовать во всех телеграммах одно и то же словосочетание, приведенное в инструкции всего лишь в качестве примера – «SONNENSCHEIN». Операторы с несколько большим воображением использовали слово «MONDSCHEIN».

Своеобразным рекордом явилась фраза, насчитывавшая 42 знака:

DONAUDAMPFSCHIFFSFARTSGESELLSCHAFTSKAPIT? N.

В случае правильного использования режим «Wahlwerter» конечно же затруднял, но не исключал возможности дешифрования сообщения.

9 апреля 1943 года после продолжительной полосы неудач к шведским криптоаналитикам пришел некоторый успех – им удалось дешифровать ряд сообщений, переданных по кабельным линиям связи и зашифрованных с использованием устройства «SZ40», созданного немецкой фирмой «Lorenz». В июне и сентябре того же года были также вскрыты сообщения, зашифрованные соответственно устройствами «SZ40» и «SZ42», но переданные по каналам радиосвязи.

Однако уже в мае немцами были введены столь радикальные изменения в процедуры шифрования, что систематическое вскрытие и чтение перехватываемых сообщений стало практически невозможным. Численность криптоаналитического подразделения была сокращена, в нем осталась лишь небольшая группа специалистов, которой были поручены как криптоанализ новых шифров, так и дешифрование ранее перехваченных, но не вскрытых по каким-либо причинам немецких телеграмм.

В течение года на смену шифровальным машинам «Т-52А/В» и «С» пришли их более поздние модификации D и E. Все

предпринятые шведскими криптоаналитиками усилия оказались напрасными – им так и не удалось проникнуть в тайны этих шифровальных машин, в которых, в отличие от предыдущих моделей, формирование ключевой последовательности происходило при нерегулярном движении ключевых колес.

В этом же году немцы стали использовать на линиях связи новую машину под кодовым обозначением «Y», однако и здесь дешифровальщиков постигла неудача.

В конце сентября, когда участь Финляндии в войне с Советским Союзом была уже предрешена, финское командование организовало операцию «Стелла Поларис» по эвакуации из страны техники и специалистов радиоразведки. В порты Швеции прибыли четыре судна, на борту которых находилось около 750 специалистов радиоразведки и криптоанализа со своими семьями. На этих же судах было доставлено большое количество аппаратуры радиоразведки и документов по кодами шифрам иностранных государств. Однако, не ожидавшие такого притока специалистов радиоразведки из Финляндии, шведы не оправдали надежд своих финских коллег. Только 15 финских специалистов были приняты на работу в шведскую «FRA». Вместе с тем, заинтересованное в приобретении ценного опыта своих зарубежных коллег, руководство «FRA» выкупило у финской стороны значительное количество радиоаппаратуры и документов радиоразведки и криптоанализа. Шведской казне это удачное приобретение обошлосьв сумму 252 875 крон.

Сегодня Радиоуправление национальной обороны «FRA» – это гражданское ведомство, подчиняющееся Министерству обороны Швеции, занимается радиоразведкой. Состоит из 7 отделов:

– сбора данных,
– обработки,
– формирования отчетов,
– системы электронной разведки,
– системного развития,
– системного сопровождения
– административного.

«FRA» создало и использует базу данных «Titan», где хранятся записи телефонных переговоров, интернет-трафика и данных электронных транзакций, перехваченных в международных коммуникациях. «Titan» содержит персональные данные, в том числе, имена, адреса, телефоны, номера социального страхования, а также политические взгляды, этническое происхождение и другие личные конфиденциальные данные.

Сбор данных телефонного трафика начался в 1993 году,

а интернет-трафика – в 2000 году. Срок хранения данных в базе составлял 18 месяцев, но 14 октября 2009 года в законодательство были внесены поправки, согласно которых этот срок был сокращен до 12 месяцев.

В распоряжении «FRA» есть несколько центров радиоперехвата на территории Швеции, корабль «Орион» и 2 самолета-шпиона «Гольфстрим IV».

Федеральная разведывательная служба Швейцарии использует секретную систему РЭР «Onyx», которая предназначена для перехвата военных и гражданских коммуникаций (электронная почта, факс и телефонные звонки).

«Onyx» – аналог систем «Echelon» и «Frenchelon», но имеет гораздо меньшие масштабы. Введение системы в эксплуатацию был начат в 2000 году первоначально под названием «SATOS-3» и завершён в конце 2005 года. Первоначальные системы «SATOS-1» и «SATOS-2», предназначенные для перехвата факсовых сообщений, были введены в действие в 1992 году.

Задачей «Onyx» является мониторинг коммуникаций, включая телефонные переговоры, передачу факсовых и интернет-сообщений с помощью спутников. Система использует списки ключевых слов для фильтрации контента передаваемых сообщений, представляющей интерес для разведки.

Выбор ключевых слов для фильтрации должен быть одобрен независимой комиссией. Система не должна контролировать внутренние коммуникации, при этом допускается мониторинг сообщений, которыми швейцарские абоненты обмениваются с иностранными.

Долгое время «Skype» считался одним из самых защищенных сервисов «VoIP» (интернет-телефония). Официально подтвержденных разработчиком случаев расшифровки и/или перехвата данных в «Skype» не было зафиксировано примерно до 2008 года.

Тогда правоохранительные органы Австрии на встрече с провайдерами сообщили, что провели «законный перехват IP-трафика». Аналогичное заявление прозвучало и от представителя органов внутренних дел Австралии. Кроме того, о наличии решений для прослушки «Skype» объявили власти Швейцарии.

4. Радиоразведка Британии

Удивительно, но в отличие от других великих держав Великобритания до Первой Мировой войны формально не имела организованных структур радиоразведки. В период войны с бурами (1899—1902) британцы приобрели некоторый опыт защиты телефонных коммуникаций от прослушки и даже пытались заниматься перехватом и дешифровкой переговоров противника.

Только в 1909 году было создано Разведывательное управление (далее – РУ) Правительственного комитета обороны Великобритании. В связи с финансовыми и кадровыми сложностями поддержания нескольких параллельных спецслужб РУ Комитета обороны было слито с Главным управлением разведки Сухопутных войск, которое на тот момент имела в составе 19 функциональных подразделений.

Каждое подразделение имело буквенно-цифровой код «MI№» (англ. Military Intelligence – военная разведка), где № – номер подразделения. Например, «MI1» – шифровальное подразделение, причем «MI1b» – секция дешифровки сообщений противника, а «MI8» – подразделение радиоперехвата.

В октябре 1914 года в Адмиралтействе была сформирована военно-морская криптослужба Великобритании, которая взялась за дешифровку накопившихся перехваченных немецких зашифрованных радиограмм. В середине ноября вся криптоаналитическая группа перебралась в большую комнату №40, расположенную в старом здании Адмиралтейства.

Располагалась она очень удачно – находилась близко к оперативному отделу, получавшему от группы дешифрованные радиограммы противника, и в стороне от других помещений Адмиралтейства. Название «комната 40» (англ. Room 40) оказалось настолько удобным и нейтральным, что вскоре стала общепринятым названием этого подразделения.

С ростом объёма вражеской шифропереписки «комната 40» перестала просто направлять отредактированные материалы радиоперехвата оперативному управлению Адмиралтейства, а стала посылать туда ежедневные сведения, которые включали криптоаналитическую, пеленгационную, радиоэлектронную и другую разведывательную информацию.

В 1915 году британский капитан Р. Стэнли (в прошлом профессор Белфастского университета) создал аппарат, который позволял индуктивным способом перехватывать информацию с проводов на расстоянии до 100 метров от них. Вскоре удалось

создать приёмник, «перехватывающий» информацию на расстоянии до 100 метров от них.

В 1916 году британские военно-морские дешифровальщики сумели добиться еще более впечатляющего успеха. В феврале 1917 года они прочли дипломатическую шифртелеграмму, которую министр иностранных дел Германии Артур Циммерман отправил немецкому послу в Мексике. Содержание этой телеграммы было предано публичной огласке в марте 1917 года, что стало одним из побудительных мотивов для вступления США в войну на стороне Великобритании.

1 ноября 1919 года «комната 40» была объединена вместе с бюро криптоанализа Директората военной разведки «MI1b» (англ. Military Intelligence), в результате чего при Адмиралтействе была создана правительственная школа кодов и шифров «GC&CS» (англ. Government Code and Cypher School).

Главной задачей правительственной криптошколы (далее – ПКШ) было обеспечение шифрованной связью всех подразделений Правительства, но была также ещё и тайная директива на «изучение методов шифрсвязи иностранных государств». Поскольку ее основная работа была связана с дипломатической перепиской, по инициативе Лорда Керзона она была передана из Адмиралтейства в МИД.

В связи с необходимостью концентрации усилий на раскрытии немецкой шифровальной машины «Энигма» в 1939 году ПКШ переехала в городок Блетчли Парк (англ. Bletchly Park) неподалёку от Лондона. Официально она стала называться «Школой кода и шифра в Блетчли Парке» (англ. Code and Cipher School at Bletchly Park) и получила кодовое имя «Станция Икс» (англ. *Station* X).

В июне 1937 года в разведывательном управлении ВМФ Великобритании решили создать оперативно-информационный центр для военного времени. Для этого капитан-лейтенант Норман Дэннинг был направлен на 3 недели в ПКШ, чтобы досконально изучить, как совместно работают специалисты радиоперехвата и дешифровки.

Возвратившись в Адмиралтейство, Дэннинг решил усилить радиопеленгаторную службу и службу радиоперехвата «Y» настолько, чтобы обеспечить возможность более глубокого изучения всех каналов радиосвязи противника. Это случилось как раз тогда, когда в гражданской войне в Испании начали принимать участие итальянские подводные лодки (далее – ПЛ).

После настойчивых ходатайств перед руководством Адмиралтейства Дэннинг наконец получил для своего подразделения 3 комнаты, в которых были размещены

специалисты радиосвязи. В одной из комнат на картах и планшетах велась прокладка текущих переходов кораблей и судов.

Другая комната была оборудована телефоном с автоматическим шифровальным устройством и пневматическими почтовыми трубопроводами, связывавшими центр с военной регистратурой, через которую проходили все телефонограммы, телеграммы и радиограммы. Так появился оперативно-информационный центр.

Материалы радиообмена противника, которые накапливались в Блетчли Парке, поступали в телетайпную комнату, откуда вручную направлялись в разные подразделения. Все данные станций радиопеленга, расположенных на территории Великобритании, координировались в одном или двух пунктах и передавались по телетайпу и пневматическим трубопроводам в оперативно-информационный центр. Данные зарубежных станций радиопеленга поступали по радиоканалам в военную регистратуру, откуда вручную направлялись в оперативно-информационный центр.

Если британская радиоразведка снова смогла стать эффективной против отлично подготовившегося к радиовойне противника, то это произошло в значительной мере благодаря усилиям и настойчивости тех людей, которые вели правильную кадровую политику.

Так, к концу лета 1939 года необходимо было создать новую военно-морскую службу из гражданских радиотелеграфистов, которыми можно было бы укомплектовать станции радиоперехвата «Y» в Великобритании и за рубежом. Принятые радисты должны были уметь перехватывать и записывать радиообмен радиостанций противника. Без достаточного резерва хорошо подготовленных специалистов такого профиля не смог бы начать функционировать важнейший отдел оперативной разведки.

От результатов работы таких специалистов зависела вся система обнаружения и слежения за движением кораблей и ПЛ противника с помощью радиопеленга. От их работы зависела также обеспеченность «сырьем» британской, а позже и американской дешифровальной службы. К 1938 году станции радиоперехвата оставались еще не укомплектованными нужными специалистами при наличии не менее 30 уже работавших радиотелеграфистов ВМФ.

Так, например, станция радиоперехвата в Гибралтаре была закрыта из-за нехватки радистов, а в то же время, исходя из потребностей военного времени, морская разведка строила для

себя несколько новых станций «Y». При этом было очевидно, что если начнется война, необходимость укомплектования радистами кораблей флота будет рассматриваться как первоочередная. И это наверняка приведет к тому, что выход из положения будут искать за счет специалистов на станциях «Y».

На состоявшемся в мае 1938 года совещании заинтересованных сторон решили, что наилучший выход из положения заключается в том, чтобы создать при Адмиралтействе гражданскую береговую радиотелеграфную службу. По штату она должна содержать не менее 180 человек по образцу и подобию служб, существовавших в ВВС и сухопутных войсках.

В соответствии с законами о военном положении 1939 года задачами вновь создаваемой военной службы радиоперехвата были обнаружение и ликвидация незаконных радиостанций в Великобритании, принадлежащих вражеским агентам или другим лицам, не имеющим лицензии на соответствующую деятельность. Эта служба радиоперехвата получила кодовое название «MI8».

К работе «MI8» был привлечён президент общества радиолюбителей Великобритании Артур Уоттс, который служил аналитиком в «Комнате 40» во время Первой Мировой войны. Он, в свою очередь, стал формировать команду добровольцев-радиоперехватчиков «VIs» (англ. Voluntary Interceptors) из круга радиолюбителей.

Радиолюбители идеально подходили для такой работы, поскольку они были широко распространены по всей стране. Каждому радиоперехватчику была поставлена конкретная задача – осуществлять ежемесячно необходимый минимум радиоперехватов. Многим из них были выданы специальные удостоверения личности «DR12», что позволило им входить в помещения, откуда велись несанкционированные радиопередачи.

Набор радиоперехватчиков шёл медленно, но в течение 3-х месяцев 50 добровольцев выявили более 600 передатчиков, как правило, расположенных в стране. Немецкая агентура в Великобритании была рагромлена, некоторые из шпионов казнены, а значительную их часть британские спецслужбы использовали для работы в качестве двойных агентов в операции «Дабл Кросс».

«MI8» также создала сеть станций радиопеленга в отдаленных уголках Британских островов с целью определения местоположения нелегальных радиостанций. К маю 1940 года стало ясно, что изначально поставленная задача службы

радиоперехвата выполнена.

В 1941 году Военное ведомство разместило оперативно-информационный центр в Хэнслоуп Парке в графстве Бакингемшир (80 км от Лондона). В том же году после некоторого внутриведомственного конфликта контроль над «MI8» был передан «MI6». К этому времени объем радиоперехвата достигал 10 тысяч сообщений в день, которые передавались для дешифровки в Блетчли Парк.

При этом специалисты «MI8» сумели раскрыть некоторые шифры немецкой военной разведки раньше, чем это сделали их коллеги в Блетчли Парке. Служба радиоперехвата хорошо финансировалась и получила в своё распоряжение новую центральную радиостанцию в Хэнслоуп Парке, названную как Специальная группа связи №3 «SCU3» (англ. Special Communications Unit №3).

Служба радиоперехвата работала круглосуточно и ожидала появления в эфире радиосигналов противника. Организованная широкая сеть разбросанных по всему миру коротковолновых (далее – КВ) радиопеленгаторов союзников была готова засечь любой радиосигнал, каким бы непродолжительным он ни был, и передать его координаты в Адмиралтейство, которое, в свою очередь, предупредит свои боевые корабли и разведывательную авиацию дальнего действия.

Обнаружение и определение места кораблей и ПЛ противника с помощью радиостанций перехвата «Y» был наиболее успешным видом деятельности военно-морской разведки Великобритании. Перехватив радиосигнал противника, эти станции немедленно передавали радиочастоту станциям радиопеленга, после чего они пеленговали работающую радиостанцию с нескольких различных направлений.

Точка пересечения пеленгов на карте указывала на приблизительное местонахождение вышедшего в эфир корабля или ПЛ. Точность определения места зависела от погоды и условий проходимости радиоволн. В арктических районах такой метод давал менее точные результаты, однако чаще всего они были вполне достаточными, чтобы определить небольшой (скажем, триста квадратных миль) район поиска для самолетов или группы кораблей, выходивших туда по сигналу оперативно-информационного центра.

Как свидетельствуют архивные документы немецкого ВМФ, комбинация данных, обеспечиваемых КВ радиопеленгом, всегда была гибельной для немецких кораблей и ПЛ. Возможность расположить станции радиоперехвата и радиопеленга на многочисленных зарубежных базах позволила британцам

добиться решающих преимуществ на таких морских театрах, как Атлантический и Индийский океан.

Важным вспомогательным источником информации в радиоразведке являлись характерные черты радиотелеграфистов противника, особенно на ПЛ. Длительная практика наряду с техническим устройством, предложенным Объединенным комитетом радиоразведывательных служб «Y» позволила изучать и распознавать характерные признаки работы на ключе отдельных радиотелеграфистов.

Сигналы радиста записывались на специальной ленте, а затем с помощью точнейшего измерения знаков определялись индивидуальные характеристики радиста, позволявшие опознавать его так же, как и по отпечаткам пальцев. Этот метод «радиоотпечатков» пальцев оказался особенно эффективным и полезным в борьбе с ПЛ противника, на которых наряду с молодыми радистами, как правило, имелся один опытный для передачи особо важных радиограмм.

Опознавание «почерка» такого радиста в течение всего периода патрулирования ПЛ позволяло прокладывать ее путь на карте обстановки, которую вели на посту слежения за движением ПЛ. Таким образом можно было узнать намерения и тактику противника и даже количество лодок, используя для этого и другую информацию, накопленную в досье на каждую ПЛ.

В целях предотвращения атак ПЛ использовалось и еще одно средство радиоразведки, которое обеспечивало кораблям охранения конвоев неоценимую тактическую информацию. Дело в том, что для навигационных целей некоторые корабли охранения были оснащены средневолновыми (далее – СВ) радиопеленгаторными станциями.

Из захваченных в 1940 году документов противника оперативно-информационный центр сделал вывод, что при проведении согласованных атак конвоев группы немецких ПЛ используют для связи между собой СВ радиостанции.

Поскольку детали всей процедуры наведения ПЛ с помощью такой связи были известны, с января 1941 года на кораблях охранения начали нести вахту с целью прослушки СВ радиообмена немецких ПЛ с тем, чтобы на основе полученных материалов разработать соответствующую систему предупреждения об опасности атак ПЛ.

К сентябрю 1942 года такая система была введена, и ни один атлантический конвой не выходил в море без кораблей охранения, оборудованных СВ пеленгаторной станцией. Однако основным противником немецких ПЛ по-прежнему оставался КВ радиопеленгатор, дававший индивидуальный пеленг

на работающую станцию ПЛ.

Одна из британских военно-морских радиостанций была размещена в советском городе Полярный. К ней было прикомандировано небольшое подразделение радиоразведки, которое вместе с русскими занималось перехватом сообщений немецких ВМС. Это подразделение проработало в Полярном до декабря 1944 года и сумело добыть там ценную развединформацию о военных кораблях Германии в северных широтах, включая данные о местонахождении немецкого линкора «Тирпиц».

Чтобы добиться эффективной и слаженной работы этого вида разведки, пришлось преодолеть множество трудных проблем. Необходимо было подготовить и задействовать большое число радиооператоров на многочисленных и широко рассредоточенных радиостанциях перехвата и пеленгования. Возникло большое напряжение в каналах радиосвязи, по которым материалы станций радиоперехвата передавались в оперативно-информационный центр.

Срочную и ценную информацию станций радиоперехвата приходилось передавать в течение какого-то периода средствами имевшейся радиосети ВМФ, и без того загруженной большим радиообменом. Лишь к весне 1943 года военно-морская разведка создала свою собственную независимую радиосеть, позволившую использовать этот источник информации наиболее эффективно и с максимальной оперативностью.

Служба радиоперехвата ВВС Великобритании, контролируя радиообмен противника во Франции, обнаружила, что в радиосвязи танков с самолетами немцы используют очень высокую частоту и сопровождают ее открытым текстом. Поэтому, когда к концу лета 1940 года угроза вторжения в Великобританию стала максимальной, 9-й отдел Разведывательного управления ВМС установил на мысе Норт-Фореленд небольшую радиостанцию, укомплектовав ее гражданскими радиооператорами и несколькими лингвистами из сухопутных войск.

На базе перехваченных данных 9-й отдел пришел к заключению, что немецкие быстроходные и хорошо вооруженные торпедные и артиллерийские катера во время действий в проливе Ла-Манш и в водах Северного моря будут поддерживать радиосвязь между собой на очень высокой частоте.

На основе опыта работы норт-форелендской станции подобные станции радиоперехвата и прослушки радиопереговоров открытым текстом или с использованием простейших кодов были построены также в нескольких пунктах

на южном и восточном побережье Великобритании.

Работа этих станций обеспечила возможность оперативно-информационному центру своевременно предупреждать о возможных атаках прибрежных конвоев, что спасло много судов и жизней как раз в тот период, когда удары немецких ВВС и ВМС по конвоям у восточного побережья серьезно угрожали сорвать снабжение Лондона и южных городов страны топливом и продуктами питания.

Позднее рядовые моряки, знавшие немецкий язык и снабженные соответствующей радиоаппаратурой, включались в состав экипажей эскадренных миноносцев с целью сбора оперативной информации путем прослушки открытых переговоров противника в море.

Введение в заблуждение немцев летом 1944 года относительно точных мест высадки союзных сил вторжения в Европу было достигнуто главным образом симуляцией необыкновенно большого оперативного радиообмена в районе, расположенном на противоположном от Кале берегу Дуврского пролива, т. е. в районе, который союзники не намеревались использовать в качестве плацдарма для высадки войск.

На пике своей деятельности в 1943—44 годах в службе радиоперехвата работало более 1500 человек, большинство из которых были радиолюбителями. Более половины из них работали в качестве перехватчиков радиопередач, а многие вели изучение радиосетей противника.

Это позволяло получать информацию, важную для британских спецслужб даже в случаях, когда не удавалось дешифровать сообщения. В нескольких случаях удалось заблаговременно выявить приёмы, которые германские агенты применяли для обеспечения безопасности своих радиопередач, и принять соответствующие контрмеры.

5. Британская ШКПС

В 1946 году на базе школы в Блетчли Парке была создана Штаб-квартира правительственной связи «*GCHQ*» (далее – ШКПС) (англ. Government Communications Headquarters). Сейчас ШКПС, которая в 1953 году переехала в Челтенхем (129 километров от Лондона), с целью «прикрытия» находится в структуре британского МИД. Её руководитель является заместителем министра, но фактически это независимый орган, который подчиняется непосредственно Премьер-министру.

ШКПС отвечает за безопасность правительственных линий связи, разработку кодов и процедур с целью защиты сообщений (обеспечение секретности связи) Правительства Великобритании. Также обеспечивает планирование, контроль, координацию действий и обработку данных перехвата всех органов Министерства обороны (ВВС, ВМФ и сухопутных войск) как в стране, так и за рубежом.

ШКПС состоит из 6 управлений, важнейшим из которых является Управление сбора данных, формулирующее потребности в разведывательной информации и обеспечивающее обработку собранных сведений. Оно состоит из отделов, основными из которых являются:

– отдел «J» (специальная техническая разведка) – ведение технической разведки в странах Восточной Европы, в том числе Содружества независимых государств (далее – СНГ) (штатная численность – около 1000 служащих);

– отдел «К» (общая техническая разведка) – ведение технической разведки в других регионах земного шара;

– отдел «Н» (криптоанализ) – дешифровка данных;

– отдел «Х» (информатика) – информационный центр управления, оснащенный современными ЭВМ большой мощности типа «*CRAY»;*

– отдел «Z» (взаимодействие) – связь и взаимодействие со спецслужбами союзных государств, с которыми заключены соответствующие соглашения.

Управление организации и личного состава выполняет, в основном, административные задачи, занимается вопросами учёбы и распределения личного состава в Великобритании и зарубежом, а также назначает личный состав технической разведки в посольства.

Управление обеспечения скрытности связи отвечает за обеспечение защищённости сообщений британского правительства, разрабатывает технические директивы по защите

информации и технических средств и руководит криптологической деятельностью в государстве.

Управление планирования отвечает за разработку долгосрочной стратегии системы технической разведки (размещение станций радиоперехвата, их обеспечения и т.п.).

Управление телевещания представляет собой организацию прикрытия для сети станций радиоперехвата ШКПС, расположенных по всему миру.

Объединённая техническая служба переводов, в основном, отвечает за перевод на английский язык перехваченных сообщений любого характера (переговоры летчиков, сообщения посольств и т. п.).

Несмотря на общее сокращение вооружённых сил, численность и финансирование служб разведки и безопасности Великобритании ежегодно увеличиваются приблизительно на 2—5%. По оценкам западной прессы, штатная численность британских спецслужб сейчас достигает 20 тысяч человек, а годовой суммарный бюджет превышает 1 миллиард фунтов стерлингов.

Бывший сотрудник британской разведки «MI5» Питер Райт в своей книге «Ловец шпиона» (англ. Spy Catcher), опубликованной в 1987 году в Австралии, рассказывает о фактах добывания секретной информации за счет перехвата побочных электромагнитных излучений и наводок (далее – ПЭМИН).

Так, в 1956 году, в ходе операции под названием «Захват» (англ. Engulf) чувствительные микрофоны, тайно установленные в посольстве Египта в Лондоне, позволили британцам по звукам механического шифратора «Hagelin» получить доступ к секретной дипломатической переписке арабов в период суэцкого кризиса.

Другая, технически более сложная операция «Плотогон» (англ. Rafter) была проведена против СССР. В 1958 году британская радиоразведка перехватывала побочные излучения аппаратуры, установленной в советском посольстве на расстоянии до 60 метров, чтобы определить частоты излучения.

Третья, политически очень важная операция «Частокол» (англ. Stockade) была проведена против Франции. В 1960 году Великобритания вела переговоры о вступлении в Евросоюз, и правительству надо было знать позицию Франции в этом вопросе.

Сотрудники «MI5» постоянно перехватывали зашифрованные сообщения французских дипломатов, но раскрыть шифр не могли. Однако в определенный момент Питер Райт при анализе излучений заметил, что наряду с основным сигналом

присутствует и другой очень слабый сигнал ПЭМИН. Британские инженеры сумели настроить радиоприемную аппаратуру на этот сигнал и демодулировать его. Это оказалось открытое незашифрованное сообщение.

Шифровальная машина французов, впрочем, как и любая другая электрическая машина, имела ПЭМИН, которое модулировалось информационным сигналом еще до момента его шифрования. В результате путем перехвата и анализа ПЭМИН французской шифровальной машины, британское правительство получало всю необходимую информацию. Таким образом задача, стоявшая перед «MI5», была решена.

Основная задача британской радиоразведки решается станциями наблюдения и перехвата, расположенными как на территории Великобритании, так и за рубежом. ШКПС имеет широкую сеть станций радиоперехвата по всему миру (около 25), наибольшая из которых находится в городе Менвит-Хилл (англ. Menwith Hill) в графстве Йоркшир.

Станция, основанная в 1950-х годах и имевшая кодовое название «Полевая Станция Ф-83» (F-83), была размещена на площади более 200 гектаров. Свыше десятка параболических антенн ориентированы на геостационарные орбиты спутников систем связи.

Сначала «F-83» предназначалась для перехвата международных коммерческих коммуникаций в сети «ILC» (англ. International Leased Carrier), которая использовалась банками и фирмами для платежей. В 1970-х станцию перепрофилировали.

В рамках программ «Steeplebush I» и «Steeplebush II» она стала «снимать» информацию со спутников. На «F-83» работает 1400 инженеров, физиков, лингвистов, математиков, информационщиков и 370 сотрудников МО. «Скромная» станция «F-83» имеет штат, равный всей «MI-5», – британской службе госбезопасности.

Она не только выполняет функцию наибольшего «уха» в мире, но и служит порталом связи с группировкой англо-американских спутников-шпионов, включая главную сеть, которая контролирует Евразию.

Ежеминутно 3 спутника «Вортекс» (англ. Vortex – водоворот), висящие над экватором, передают на «F-83» разведывательную информацию в режиме реального времени. Более современные большие спутники «Магнум и Орион» (англ. Magnum & Orion) также управляются с «F-83».

«F-83» является одновременно и самим мощным узлом классического радиошпионажа. Она перехватывает сообщения, которые передаются микроволновыми линиями связи, УКВ и КВ

сигналы, которые создаются военными радиостанциями.

Для управления техническими средствами радиоперехвата, отбора и дешифрования полученных материалов используются более десятка супер-ЭВМ. Эти ЭВМ автоматически анализируют все телефонные и телеграфные сообщения, а также данные, циркулирующие в компьютерных сетях, выделяя интересующую информацию. На базе имеется также сеть контрольных постов для приема данных перехвата американских спутников радиоразведки.

Но этого, по-видимому, было недостаточно. Согласно планам модернизации базы на ее территории были дополнительно установлены 4 радиомачты высотой 30 метров каждая и 7 антенн, скрытых под обтекателями, 3 из которых высотой около 30 метров. База будет еще в большей мере насыщена ЭВМ. Только на ее модернизацию до 1993 года было выделено более 40 миллионов долларов.

В 1967 году в Корнуолле по соседству с приемной станцией спутниковой системы связи «Интелсат» ШКПС построила собственную копию этой станции для перехвата спутниковых сигналов «GCHQ Bude». За оборудование и инфраструктуру заплатило АНБ, а ШКПС взяла на себя эксплуатационные расходы и арендную плату за землю. Станция прослушивает Европу, Атлантический и Индийский океаны и примыкающие к этим регионам государства.

Станции за рубежом находятся в Гибралтаре, Омане, Германии, Турции, Ботсване, на острове Вознесения и Кипре. Впрочем, некоторые из этих станций перехвата Великобритании пришлось закрыть (например, в Гонконге) или «залегендировать» в соответствии со сложившимися обстоятельствами.

Станция, находившаяся в Мешхеде около советско-иранской границы, во время народных волнений в Иране подверглась нападению. В результате четверо ее сотрудников были убиты, а сама станция прекратила свое существование.

Тщательно замаскированные подразделения РЭР – «уши» дешифровальной службы ШКПС – располагаются в некоторых зарубежных представительствах Великобритании. Есть такое подразделение и в британском посольстве в Москве.

После терактов 11 сентября 2001 года Великобритания вслед за США выделила значительные финансовые средства для повышения эффективности своих спецслужб. В результате, если в 2001 году их бюджет составлял 2 миллиарда долларов, то к 2007 году он вырос более, чем вдвое, – до 4,2 миллиарда. ШКПС получил на расходы больше всех остальных спецслужб – 1,6 миллиарда долларов.

На дополнительно выделенные средства, в первую очередь, было решено срочно модернизировать инфраструктуру ШКПС. С этой целью в Челтнеме было начато возведение современного комплекса зданий штаб-квартиры взамен прежнего, который находился здесь же. Строительство было закончено в конце 2003 года и обошлось английским налогоплательщикам в 660 миллионов долларов.

Переезд сотрудников ШКПС в новую штаб-квартиру состоялся в 2004 году. Первоначально планировалось, что одновременно с ними туда переедут и суперкомпьютеры, которые использовались для обработки поступавших в ШКПС разведданных. Но потом было решено оставить суперкомпьютеры на прежнем месте, чтобы ни на секунду не прерывать процесс добывания ценной информации.

Поэтому помимо 120 миллионов долларов, выделенных на переезд, было дополнительно израсходовано 60 миллионов долларов на прокладку оптоволоконного кабеля для связи суперкомпьютерного центра с новой штаб-квартирой. Планировалось, что по мере износа и старения суперкомпьютеры будут демонтироваться, а взамен них в новой штаб-квартире будут устанавливаться более современные и быстродействующие.

Нельзя оставить без внимания и заявления американца Эдварда Сноудена, который с двумя миллионами секретных файлов АНБ сбежал из США и 1 августа 2013 года получил временное убежище в России. Он работал в АНБ, информационном отделе ЦРУ и консалтинговых компаниях, сотрудничающих с АНБ, и имел допуск не только к совершенно секретной, но и специальным разведданным, содержащим технические детали операций США и их союзников по перехвату и прослушке.

Сноуден предал огласке секретную информацию АНБ, касающуюся прослушки телефонных разговоров и перехвата электронных сообщений миллиардов людей из десятков стран. В результате свидетельств Сноудена стало известно о существовании секретных разведывательных программ, используемых в США, Великобритании, Франции, Швейцарии, Швеции, Китае и Индии.

Генеральный директор Бюро по безопасности и борьбе с терроризмом Великобритании Чарльз Фарр признал в суде, что перехват информации в «Facebook», «Twitter», «Google» и «YouTube» в Великобритании производится на вполне законных основаниях, поскольку все эти интернет-сервисы классифицируются как «внешние коммуникации».

По данным Сноудена непосредственно ШКПС разработала

и применяет следующие секретные компьютерные разведывательные системы и программы.

1. «**Impact Nominal Index**» (Номинальный индекс воздействия) – компьютерная система, предназначенная для полиции и других силовых структур Великобритании, которая позволяет оперативно навести справки об интересующих лицах.

Система была разработана в 2006 году в рамках реализуемой МВД программы «Impact» с учётом рекомендаций, высказанных представителями полиции после убийства двух школьниц в Сохеме в 2002 году. Разработчиком система была компания «Web Technology Group».

Система представляет собой, по сути, базу данных, содержащую список имен и соответствующие даты рождения людей, которые по каким-либо причинам фигурировали в полицейских протоколах. Эта программа обеспечивает оперативный и эффективный доступ к информации, которая очень важна для борьбы с преступностью, особенно во время критических ситуаций.

2. «**Karma Police**» (Полиция Кармы) – программа для сбора метаданных интернет-пользователей, задуманная в 2007 году и запущенная с 2009 года. Представители ШКПС характеризуют программу как крупнейшую в мире по масштабам интеллектуального анализа данных в интернете.

«Karma Police» предназначена для описания профилей, характеризующих индивидуальные особенности (привычки) пользователей интернета. Она извлекает информацию из межконтинентальных кабелей передачи данных, пропускающих 25% всего мирового интернет-трафика. Собранные метаданные содержат записи имён пользователей, пароли и адреса посещённых веб-сайтов.

«Karma Police» используется, по-видимому, без контроля со стороны правительства. К 2009 году благодаря использованию программы были получены и хранятся описания более 1,1 триллиона посещений сайтов. При этом в 2010 году программа собирала ежедневно более 30 миллиардов записей, а к 2012 году эта цифра достигла 50 миллиардов.

«Karma Police» была создана, чтобы обеспечить одно из следующих действий: а) просмотр профиля посещения веб-страниц для каждого видимого пользователя в интернете, или б) просмотр данных пользователей для каждого видимого веб-сайта.

3. «**Muscular**» (Сильный) – программа, используемая совместно с АНБ для взлома коммуникаций между дата-центрами «Yahoo» и «Google».

Программа является одной из составляющих пакета

компьютерных программ слежения, известного под названием «WindStop», в который входит по меньшей мере 4 программы. За 30-дневный период – с декабря 2012 по январь 2013 года, программа произвела сбор 181 миллионов записей.

Этот объём является незначительными по сравнению с действием другой программы из пакета «WindStop», известной под названием «Incenser» и кодом «DS-300», которая за тот же период собрала более 14 миллиардов записей.

«Muscular» ежедневно пересылает миллионы записей из внутренних сетей «Yahoo!» и «Google» в хранилище данных в штаб-квартире АНБ. Программа работает через точку доступа, известную под кодовым названием «DS-200B», которая находится за пределами США, с использованием неизвестного оператора связи, который обеспечивает негласный доступ к данным для АНБ и ШКПС.

Из-за огромного объёма передаваемых данных «Muscular» ставит особые задачи перед подразделением «SSO» (англ. Special Source Operations – операции специального источника) АНБ.

Например, когда «Yahoo!» решила переместить большое количество электронных почтовых ящиков в своих дата-центрах, база первичных интернет-данных АНБ «Pinwale» была быстро перегружена по мере поступления данных от «Muscular».

С использованием «Muscular» тесно связаны программы «Incenser» и «Turmoil». В частности, «Turmoil» представляет собой систему обработки данных, собранных «Muscular».

Эксплуатация «Muscular» стала возможна в силу того, что «Google» передавала данные внутри своего частного облака в незашифрованном виде и, соответственно, использовала протокол SSL для внешних соединений.

4. «**Royal Concierge**» (Королевский консьерж) – это программа ШКПС, которая следит за электронными заказами клиентов, сделанными в некоторых отелях по всему миру.

5. «**Squeaky Dolphin**» (Пискливый Дельфин) – программа сбора и анализа данных из социальных сетей, позволяющая в режиме реального времени отслеживать просмотры видеороликов на «YouTube», «лайки» в «Facebook», посещения сервиса «Blogger» и «Twitter».

«Squeaky Dolphin» может быть дополнена доступными коммерческими аналитическими программами, которые позволят определить, например, какие именно видеосюжеты пользуются популярностью у жителей конкретных городов. Интерфейс программы разработан американской компанией «Splunk».

Презентация «Squeaky Dolphin», продемонстрированная аудитории АНБ, содержит упоминание, что программа

«не ориентирована на отслеживание действий отдельных лиц, а фиксирует лишь общие тенденции». Тем не менее, уже в 2010 году ШКПС использовала незашифрованные данные из «Twitter» для определения конкретных пользователей по всему миру для ведения целенаправленной пропаганды.

6. «**Tempora**» – программа перехвата информации, передаваемой по волоконно-оптическим линиям связи и магистральным каналам Интернета, запущенный в действие осенью 2011 года и используемый ШКПС совместно с АНБ.

Два основных компонента программы, которые называются «Mastering the Internet» и «Global Telecoms Exploitation», ведут сбор данных из перехватов телефонных разговоров и интернет-трафика, записей в «Facebook» и личных профилей интернет-пользователей.

В работе программы используется более 200 оптоволоконных кабелей, полученные данные сохраняются в течение 3-х дней, метаданные хранятся в течение 30 дней.

По утверждениям некоторых британских официальных лиц, объем метаданных в ШКПС больше, чем в АНБ. Около 850 тысяч человек имеют допуск для доступа к данным. В мае 2012 года 300 аналитикам ШКПС и 250 аналитикам АНБ было поручено обработать массив накопленных данных.

Создание «Tempora» было возможно только в секретном партнёрстве с коммерческими компаниями, которые были описаны в документах ШКПС как партнёры по перехвату. Персоналу ШКПС было приказано скрыть происхождение данных в своих докладах из опасений «политических последствий на высоком уровне».

Запуску «Tempora» предшествовал 3-летний испытательный период на станции радиоперехвата в Корнуолле. К лету 2011 года была создана сеть из 200 линий передачи данных, каждая с пропускной способностью 10 гигабит в секунду.

Аналитики АНБ участвовали в тестовых испытаниях, и «Tempora» была введена осенью 2011 года, при этом сбор данных шёл совместно с АНБ. В настоящее время ШКПС ведёт техническую модернизацию каналов передачи данных, планируя довести их пропускную способность до 100 гигабит в секунду.

В 2012 году ШКПС отчиталась о «новых возможностях доступа» к компьютерам «Google», однако масштаб проекта и пути получения информации остались неизвестными.

Поиски методов дешифровки имеют особое значение для ШКПС. Стратегическое преимущество управления, которое оно получило в связи со своей программой «Tempora», позволявшей

спецслужбам подключаться непосредственно к трансатлантическим оптоволоконным кабелям ведущих телекоммуникационных корпораций, оказалось под угрозой, поскольку сейчас все большее число компаний зашифровывают свой трафик в ответ на требования пользователей гарантировать безопасность их личной информации.

Без должного внимания, как говорится в документе ШКПС от 2010 года, «полезность британской радиоразведки снизится, поскольку сейчас информационный поток стремительно меняется, разрабатываются новые приложения, и шифрование становится все более распространённым».

Из документов следует, что первоначальная цель «Edgehill» заключалась в дешифровке зашифрованного трафика 3-х крупных интернет-компаний (их названия не раскрываются) и 30 типов виртуальных корпоративных сетей, используемых бизнесом для защиты удаленного доступа к их системам. К 2015 году ШКПС начала взламывать коды, используемые 15 крупнейшими компаниями и 300 типами виртуальных корпоративных сетей.

Ещё одна программа, которая носит название «Cheesy Name», была направлена на поиски шифровальных ключей, известных как сертификаты, которые можно взломать при помощи сверхмощных компьютеров ШКПС. В рамках проекта «Edgehill» аналитики также занимались поиском способов проникнуть в сети ведущих провайдеров почтовых веб-сервисов.

В квартальном отчете от 2012 года говорится, что группа аналитиков «продолжает изучать» основных интернет-провайдеров «Hotmail», «Google», «Yahoo» и «Facebook», и что «в этом квартале их внимание в первую очередь сосредоточено на „Google“ в связи с разработкой новых возможностей доступа».

Чтобы сохранить свои преимущества, ШКПС создало «Оперативную группу агентурной разведки». Эта группа занимается обработкой информации, полученной непосредственно от источников и агентов, работающих под прикрытием. Согласно внутриведомственным документам, эта группа «отвечает за поиск, вербовку и поддержку тайных агентов в мировой телекоммуникационной индустрии».

«Она позволяет ШКПС решать наиболее сложные задачи», – говорится в докладе. Эксперты предупреждают, что деятельность АНБ и ШКПС, направленная на взлом шифровальных систем, может иметь негативные последствия для всех интернет-пользователей.

14 июля 2014 года Сноуден в интервью «The Guardian» перечислил список программ, которые ШКПС использует для управления интернет-трафиком:

– «Gateway» (Шлюз) – увеличение нагрузки на сайт,

– «Clean Sweep» (Чистка) – маскирует записи на стене в «Facebook» для отдельных стран,

– «Spring Bishop» (Весенний Епископ) – поиск по личным фотографиям в «Facebook»,

– «Scrapheap Challenge» (Скрытая Проблема) – подмена писем от пользователей «BlackBerry»,

– «Underpass» (Туннель) – изменение результатов онлайн-опросов.

Благодаря откровениям бывшего техника Управления безопасности коммуникаций (далее – УБК) Министерства национальной обороны Канады Майка Фроста, стало известно, что в 1980-е годы ШКПС по заданию Премьер-министра Маргарет Тэтчер использовал УБК, чтобы прослушивать 2-х собственных министров, которые были тогда «оппозиционерами».

Один из прослушиваемых чиновников был министр иностранных дел Фрэнсис Пим, который курировал ШКПС и военную разведку «MI6», а другой – заместителем Премьер-министра и министром внутренних дел Уильямом Уайтлоу.

В 2016 году Великобритания приступила к реализации многомиллионного проекта по созданию шпионского центра нового поколения, который будет заниматься перехватом всего электронного траффика внутри страны.

Новое учреждение будет называться Правительственным Центром технической поддержки «GTAC» (англ. Government Technical Assistance Center). Он будет располагаться в здании контрразведки «MI5», которая занимается внутренней безопасностью в стране.

Создание центра проходит в рамках принятого в 2016 году закона о полномочиях следствия (англ. Regulation of Investigatory Powers Act). Он под предлогом необходимости борьбы с терроризмом наделяет ряд спецслужб широкими возможностями по слежке за подданными, в том числе правом «взламывать» телефоны и компьютеры, массово собирать персональные данные и т. п.

В соответствии с данным законом все провайдеры страны должны будут с 2017 года собирать списки посещённых пользователями сайтов и хранить их на протяжении 12 месяцев и предоставлять полиции доступ к этим данным. Британских провайдеров обяжут протянуть выделенную линию в офис спецслужбы, для того чтобы она могла проводить мониторинг всего траффика, проходящего через данного провайдера.

Пользователи будут обязаны, по первому требованию органов правопорядка, сообщать им пароли для дешифровки защищенных

сообщений. При этом закон требует получения органами соответствующей санкции. Британское правительство утверждает, что и новый закон, и новый центр тотального электронного надзора поможет в борьбе с компьютерной преступностью в собственной стране.

В 2016 году решением Трибунала по вопросам следственных полномочий «IPT» (англ. Investigatory Powers Tribunal) «эксплуатация компьютерных сетей», в том числе односторонняя инициатива подключения микрофонов и видеозаписи на технических устройствах, признана легальной. Трибунал также наделил ШКПС правом формировать выборки по критериям прослушки, например, «подключиться ко всем телефонам в Бирмингеме».

Решение Трибунала вызвало протест правозащитных организаций. По мнению активистов, британские спецслужбы слишком усердствуют в своем вторжении в частную жизнь граждан и тем самым нарушают европейские законы. Сноуден уже охарактеризовал практику работы британских спецслужб, заявив, что она «даже хуже, чем слежка в США».

Решение Трибунала не подлежит апелляции. Он является единственным органом правосудия в Великобритании, который рассматривает жалобы на действия служб разведки.

Ранее правительство Великобритании утвердило новый законопроект о следствии и сыскной деятельности, известный также как «кодекс сыщика». Новый законопроект позволят ШКПС получать разрешение на доступ к любым типам контента связи и данных в массовом порядке.

ШКПС и правительство Великобритании утверждают, что использование технологий электронного слежения является законным в рамках национального законодательства и не нарушает прав человека. Согласно решению Трибунала практика взлома компьютеров и телефонов без ведома их владельцев совместима с Европейской конвенцией о правах человека.

Министр иностранных дел Великобритании Филип Хэммонд приветствовал решение Трибунала: «Способность использовать компьютерные сети играет ключевую роль в нашей способности защитить британскую общественность».

Однако сотрудник благотворительной организации «Privacy International» Скарлет Ким заявила по этому поводу: «Мы разочарованы приговором Трибунала, который признал практику взлома компьютеров правительством законной на основе расширительного толкования закона 1994 года, когда интернет и мобильные технологии были еще в зачатке».

В отчёте ШКПС за последний фискальный год указано, что в 2015—16 годах она потратила на кибероперации 24% своего бюджета – это самая большая статья расходов у разведчиков. За ней следует борьба с терроризмом (контртеррористические операции) – 23% бюджета.

На 40-й странице отчёта говорится о том, что в последние годы ШКПС «не справляется с наймом и удержанием подходящего и достаточного кадрового состава для заполнения штатных вакансий технических специалистов, поскольку ведомству неизбежно приходится конкурировать с крупными технологическими компаниями, которые платят гораздо больше».

В данный момент ШКПС испытывает серьёзные проблемы с наймом и удержанием персонала, а именно, специалистов по компьютерной безопасности. Сейчас спрос на таких сотрудников особенно высок.

6. Радиоразведка 3-го Рейха

В конце 1912 года в немецком Генштабе была создана самостоятельная служба разведки и контрразведки, получившая официальное название «III-b». Созданное в ней подразделение радиоразведки стало одним из ключевых факторов поражения 1-й и 2-й русских армий в Восточно-Прусской операции 1914 года. Огромную роль в ходе и исходе операции сыграл радиоперехват.

Перехват русскими радистами радиограмм 17-го и 20-го корпусов 8-й немецкой армии установил, что главные силы немцев сосредоточились за рекой Ангерапп. Это обстоятельство во многом повлияло на результат Гумбинненского сражения 7 августа, в котором потерпели тяжелое поражение 2 корпуса немецкой армии. Вечером 7 августа командующий армией генерал фон Притвиц, подведя итоги сражения, посчитал его проигранным.

С 11 августа в руки немецкого командования регулярно начали поступать русские оперативные радиограммы, а также боевые приказы 2-й русской армии. Начиная с этого дня немецкое командование действовало в строгом соответствии с известными ему планами своего противника.

Так, 2 перехваченные 12 августа радиограммы раскрыли как группировку 1-й и 2-й русских армий, так и планы действий командующих этими армиями. Немецкие генералы действовали наверняка, в то время как русские основывались, прежде всего, на догадках.

Например, если сведения авиаразведки, собранные к 12 августа в штабе 8-й немецкой армии, давали ее командованию очень ограниченные и отрывочные данные о наступлении 6-го русского армейского корпуса севернее Ортельсбурга, то русские радиограммы восполнили недостаток информации и очень помогли немцам.

Получили немцы также текст директивы фронта штабу 2-й русской армии. Прочитал противник и директиву главнокомандующего фронтом командующему 1-й русской армией о приостановке наступления, в результате чего командование 8-й немецкой армии решилось на рокировку своих войск против генерала Александра Самсонова.

А радиограмма Самсонова командованию 13-го армейского корпуса (у которого шифр отсутствовал) открытым текстом дала немцам не только полную картину оперативной обстановки, но и раскрыла план предстоящих действий 2-й армии.

Дело в том, что русские корпуса, израсходовав средства

проводной связи со своими дивизиями, уже не могли дотянуться своими проводами как до штаба армии, так и до своих соседей. Армейский штаб в этом вопросе ввиду нехватки ресурсов помочь им не мог. Поэтому уже 10 августа 1914 года проводная связь штаба 2-й армии с некоторыми корпусами была прервана.

Стали более активно использовать связь посредством искрового телеграфа. Но при эксплуатации этого нового средства связи особенно сильно сказалась дезорганизованность, которую внесла в действия связистов спешка выдвижения 2-й армии к границе.

Дело в том, что начальник шифровального бюро армии вплоть до самого начала боевых действий воздерживался от отправки в войска нового шифра, который должен был использоваться в период боевых действий. Разумеется, новый шифр радисты освоить не смогли, и поэтому часто осуществляли передачи открытым текстом.

Так, когда армии стали пытаться общаться между собой по радио, выяснилось, что армия генерала Павла Ренненкампфа уже получила новый шифр и уничтожила старый, в то время как в армии Самсонова имелся лишь старый шифр.

В результате армии разговаривали «на разных языках» – радиообмен шел разными шифрами, именно поэтому армейские рации начали работать открытым текстом. И вот здесь сыграла свою роль немецкая служба радиоразведки, которая перехватывала и передавала все русские сообщения командованию немецких войск.

Один из главных «архитекторов» победы 8-й немецкой армии в Пруссии начальник оперативного отдела штаба полковник Макс Хоффман, руководивший в тот период радиоперехватом, утверждал, что он знал всё о русских планах из прослушанных радиопереговоров.

В результате 5 русских дивизий 13-го и 15-го корпусов 2-й армии (около 30 тысяч человек при 200 орудиях) были окружены в районе Комусинского леса. В ночь на 30 августа 1914 года командующий 2-й армией генерал Александр Самсонов, находившийся среди окружённых частей, застрелился.

Таким образом, 8-я немецкая армия под командованием генерала Пауля фон Гинденбурга отразила наступление превосходящих сил 2-х русских армий в Восточную Пруссию, нанесла поражение 2-й армии и вытеснила из Восточной Пруссии 1-ю армию, что стало заметным оперативным успехом Германии в Первую Мировую войну.

Однако этим война Германии с Россией не закончилась, поэтому работа радиоразведки продолжалась, и теперь в ней

появился профессор филологии Кенигсбергского университета Людвиг Дойбнер. Он с началом войны был зачислен в немецкое народное ополчение в качестве переводчика с русского языка.

Дойбнер начал свою службу в радиоразведке с перевода перехваченных сообщений, переданных в открытом виде. По мере появления в этих текстах зашифрованных слов он пытался прочитать и их. Постепенно у профессора накопился такой опыт работы в этой области, что он смог полностью дешифровывать радиограммы противника.

В середине сентября 1914 года Дойбнер был вызван в штаб и назначен руководителем переводчиков, отобранных для обучения криптоанализу. После подготовки из них была создана штабная дешифровальная группа. Каждый вечер к 11 часам она направляла начальнику штаба 8-й армии генералу Эриху фон Людендорфу дешифрованные криптограммы.

Тот ожидал их с большим нетерпением и часто спрашивал у своих подчиненных, есть ли перехваченные документы противника. Приказы, которые Людендорф отдавал на следующий день, в значительной мере основывались на информации, полученной от дешифровщиков. Если же результаты дешифровки не доставлялись вовремя, он сам отправлялся в дешифровальную группу, чтобы выяснить причины задержки.

А когда в перехваченных и обработанных русских радиограммах не содержалось ценных данных, Людендорф выражал недовольство по поводу того, что дешифровальная группа работает недостаточно внимательно. Однако такое случалось редко.

Вскоре была установлена прямая телефонная связь между службами австрийской и немецкой радиоразведки на Восточном фронте. Австриец Герман Покорный и немец Людвиг Дойбнер совместно читали почти все русские шифровки, полученные на постах радиоперехвата.

Так, стало известно о планах русского наступления на Силезию, являвшуюся промышленным центром Центральной Европы. К концу сентября перед Гинденбургом и Людендорфом лежала информация о составе, дислокации, численности и планах русских войск. Неизвестна была только дата начала наступления, но немцы решили взять инициативу в свои руки и нанесли упреждающий удар.

В результате за успешную битву под Танненбергом и разгром русских войск в Пруссии в ноябре 1914 года Гинденбург был произведён в ранг фельдмаршала и назначен главнокомандующим немецкими войсками на Восточном фронте,

а 9 декабря 1916 года был награждён Большим крестом Железного креста.

В августе 1916 года Гинденбург стал начальником ГШ, а Людендорф стал его заместителем – первым генерал-квартирмейстером ГШ. Тогда же на французском фронте была создана «служба прослушивания» (нем. *Abhörendienst),* которая занималась перехватом вражеских сообщений и испытывала практически все известные криптосистемы в разных вариантах.

После окончания Первой мировой войны в 1919 году Германия стала Веймарской республикой и согласно Версальского Договора ее вооруженные силы «Рейхсвер» (нем. Reichswehr, Reich – государство, империя, Wehr – оборона) выполняли исключительно оборонные функции. В их состав организационно вошла служба связи и информации «III-b» (нем. Militärische Nachrichtendienst Abteilung III-b). Секретная служба занималась только защитой собственных государственных и военных секретов.

В том же году эта служба «прокололась». Так, некий «доктор Винклер», якобы доцент Высшей технической школы в Берлине и специалист в области радио, был назначен советником при шифровальном ведомстве правительства Германии. Там он быстро ознакомился со всей военной шифровальной и радиослужбой.

Для него это было тем более важно, что он тайно работал на польскую разведку. И однажды «Винклер» исчез, и с этого момента Берлину пришлось долго принимать в расчет серьезное улучшение в работе польской военной шифровальной и радиослужбы.

Весной 1920 года несколько бывших сотрудников майора Фридриха Гемппа в составе «Рейхсвера» приступили к созданию контрразведывательной службы, образованной из остатков отдела «III-b». Будущим отделом контрразведки стала армейская служба связи и информации (нем. Heeres-Nachrichtendienst).

Хотя Версальский договор разрешал отрядам связи «Рейхсвера» иметь подразделения радиоперехвата, Контрольная комиссия запретила проводить какую-либо криптоаналитическую работу. Тем не менее, в начале 1919 года 24-летний лейтенант Эрих Бушенхаген, работавший во время Первой Мировой войны в службе радиоперехвата, по собственной инициативе скрытно создал небольшое разведывательное подразделение радиоперехвата.

Свое подразделение он назвал «Добровольная служба оценки» и спокойно разместил его в доме 110 на Фридрихштрассе. Вначале оно занималось переводом незашифрованных текстов,

перехваченных из французских, английских, американских и русских источников, а также сообщений прессы и радио. Но к маю, после того, как Бушенхаген набрал несколько первых криптоаналитиков, служба предоставила руководству несколько дешифрованных сведений о России.

В феврале 1920 года служба Бушенхагена из 12 человек вошла в состав «Абвера» как Центр шифрования и скрытно переехала в здание штаб-квартиры армии на Бендельштрассе. Затем, чтобы вовремя избежать проверки инспекторов Контрольной комиссии, Центр вновь скрытно переехал теперь уже в близлежайший Грюнвальд.

Для введения в заблуждение «любопытных» здесь он разместился под вывеской «Группа газетного перевода и изучения». Помимо прочего, эта служба перехватывала переговоры контрольной комиссии, поэтому «Рейхсвер» и военные промышленники были чаще всего оповещены о предстоящем инспекционном визите.

1 января 1921 года было создано министерство «Рейхсвера», в состав которого вошла военная контрразведка под названием «Абвер» (нем. Abwehr – оборона, отражение). Организационно «Абвер» подчинялся военному министру и находился в министерстве до 1928 года в составе отдела «T3» (нем. Gruppe Abwer der Abteilung T3). «Абвер» содержал 3 подгруппы: I) разведка, II) шифрование и радиоперехват, III) контрразведка.

В том же году «Рейхсвер» отдал секретный приказ о расширении деятельности подгруппы шифрования и радиоперехвата, «Абвер-II». К концу 1925 года «Абвер-II» был тайно расширен до 32 человек и 20 радистов, обслуживающих 6 постов радиоперехвата в крупнейших городах Германии и 4 приемника, которые работали круглосуточно.

Самой важной была стационарная радиостанция и станция радиоперехвата под командованием майора фон Рихтгофена в Кёнигсберге. Она отвечала за круглосуточное радионаблюдение за всей восточной зоной, дешифрировку и взаимодействие с подгруппами «Абвер-I» и «Абвер-III».

Служба перехвата «Абвер-II» фиксировала радиопередачи дипломатических и разведывательных служб иностранных государств, в то время как на более низком тактическом уровне армейские службы перехвата имели дело с радиограммами соседних воинских частей противника.

Сухопутные войска имели батальон радиоразведки для перехвата сообщений иностранных армий, ВВС – собственную службу радиоразведки и ВМФ – собственную службу наблюдения *«B-Dienst»*, которые вели подобную работу против ВВС

и ВМФ иностранных держав.

В 1928 руководством Германии было принято решение объединить группу военной контрразведки и службу разведки ВМФ, повысив, таким образом, «Абвер» до отдела. С этого времени все мероприятия по разведке и контрразведке проводились только «Абвером», всем другим военным структурам заниматься этим, было запрещено.

В качестве непосредственных исполнительных органов в каждом из 7 военных округов (корпусов) были созданы отделения «Абвера». Они располагались следующим образом: в 1-м округе в Кёнигсберге, во 2-м – в Штеттине, в 3 м – в Берлине, в 4-м – в Дрездене, в 5-м – в Штутгарте, в 6-м – в Мюнстере и в 7-м – в Мюнхене.

К 1935 году подгруппа «Абвер-II», которая занималась радиоразведкой и дешифровкой, содержала 20 человек, а к 1940 году – более 1000. Результатом ее активной работы стал перехват радиопереговоров польских ВВС и прослушивание польской сети связи сухопутных войск. Поэтому в любой день и час «Абверу» было известно все о польских маневрах и планах польских штабов.

Помимо разведслужбы генштаба сухопутных войск, в морском генштабе была собственная служба разведки и связи, которая была оснащена всеми мыслимыми в то время техническими средствами. Здесь готовились и проводились операции германских подводных сил.

В невидимой борьбе тайных служб «Абвер» с самого начала полностью осознал огромное значение радиосвязи, которая в техническом плане далеко ушла вперед со времен Первой Мировой войны. Для систематического контроля радиопереговоров в сетях ВМФ других стран, имевших для немцев преимущественное значение, были развернуты станции дальнего радиоперехвата.

Они получили официальное обозначение станции радионаблюдения. Такая радиостанция в Киле, например, вела радионаблюдение вначале за передвижением кораблей ВМФ соседних стран – Дании и Швеции, а потом и за постоянными линиями британского адмиралтейства в Восточной Азии, Индии и Австралии. Она добилась в этом значительных успехов.

Морской генштаб в первые годы Второй Мировой войны был хорошо информирован о положении всех британских судов и кораблей, выходивших из американских портов и шедших в Великобританию, поскольку они регулярно посылали по радио шифрограммы.

Развернутая близ нью-йоркской гавани радиостанция

мощностью 110 кВт, которой владели «друзья немецкого дела», могла в течение долгого времени перехватывать эти британские шифровки, расшифровывать их и сообщать о местоположении судов немецким подводным лодкам. Уже после войны американцы утверждали, что военно-морской атташе Германии капитан I ранга Бой-Эд имел копию тайного кода британского адмиралтейства

Обычно работу и направление поиска отдельных станций радионаблюдения определяло их географическое положение в Германии. Например, станции в Кёльне, Мюнстере и Висбадене были ориентированы на запад, но были и исключения. Так, сверхмощная радиостанция в Гамбурге пользовалась правом «свободной охоты» по всему миру.

Она позволяла следить за радиопереговорами в США, в Южной Америке, на Ближнем и Среднем Востоке. Еще одна первоклассно оснащенная радиостанция была создана в 1938 году в Вене после присоединения Австрии. Отсюда теперь можно было охватить радиоразведкой всю территорию Балкан.

Необходимый для этих радиостанций персонал подбирался из числа радиолюбителей. В результате был создан штат таких первоклассных специалистов в этой области техники, каких можно было только пожелать. На радиостанции в Вольдорфе близ Гамбурга обслуживалось одновременно до 20 передатчиков. В то же время здесь работали 24 приемных устройства.

Передающие и принимающие установки были удалены друг от друга примерно на 2,5 км. На случай выхода из строя основных линий электроснабжения имелся подземный дизельный силовой агрегат. Вольдорфская радиостанция не обслуживала связь ни с какими инстанциями вермахта. Она работала исключительно в интересах связи с агентами, прошедшими специальную подготовку в гамбургском отделении абвера и разбросанными по всему миру.

Подготовка таких агентов осуществлялась в одном из пригородов Гамбурга. «Почерк» каждого агента, т. е. стиль, в котором он работает ключом радиоаппарата, записывался на пленку. Тогда тот, кто впоследствии принимал на условленной частоте первые позывные какого-то агента, должен был тщательно сопоставить запись с идущими сигналами, чтобы удостовериться, что работает именно данный агент, а не радист противника.

Немецким изобретателям удалось к тому же создать такие приемопередатчики, которые помещались в небольшом чемодане вместе с источниками питания. В годы войны эти аппараты позволяли при сравнительно небольшой мощности порядка 20—60 ватт обеспечивать устойчивую радиосвязь на невероятно

больших расстояниях.

В октябре 1937 года в структуре вооруженных сил, называемых «вермахтом» (нем. *wehr* – оборона, *macht* – сила), было сформировано подразделение разведывательной связи. Когда в феврале 1938 года служба «вермахта» была реорганизована в Верховное главнокомандование «OKW» (нем. Oberkommando der Wehrmacht), подразделение вошло в состав отдела оперативного руководства.

В это время «Абвер» вошел в состав управленческой группы по общим вопросам «OKW», а 1 июня того же года преобразован в отдел разведки и контрразведки «OKW». Подотдел «Абвер-I» отвечал за подготовку агентов-радистов, радиоперехват и дешифровку перехваченных радиограмм.

Весной 1940 года отдел оперативного руководства «OKW» стал штабом оперативного руководства, в котором появился самостоятельный отдел связи «WNV» (нем. Wehrmacht Nachrichtenverbindungen).

В составе «WNV» функционировал сектор шифров «Chi» (нем. Chiffrierabteilung), в котором работал персонал прежней подгруппы «Абвер-II». Он обеспечивал безопасность военных коммуникаций, перехват иностранной переписки и контроль над соответствующими службами сухопутных войск (нем. *heeres* – армия), ВМФ (нем. *kriegsmarine: krieg* – война, *marine* – морской) и ВВС (нем. *luftwaffe: luft* — воздух, *waffe* – оружие).

«Chi», которое имело свою группу радиоперехвата, возглавлял полковник Зигфрид Кемпф. С 1922 года началось сотрудничество с венгерскими коллегами в области радиоразведки и дешифровки. В довоенный период венгерские посты радиоперехвата покрывали всю территорию Юго-восточной Европы, поэтому немцы могли сосредоточить свои усилия на других направлениях и создать на них высокую плотность пеленгаторов и приёмников.

До начала 1942 года в дополнение к стационарному радиопеленгатору в Дании немецкая армия имела 2 группы радиоразведки. ВВС создали 1 группу и эскадрилью из 9 самолетов «Fieseler Fi 156 Storch», оборудованных средствами пеленгации, а ВМФ выделил в службу радиоразведки несколько специалистов.

С 1932 по 1939 год численность военнослужащих немецкой радиоразведки, включая «вермахт», «кригсмарине» и «люфтваффе», увеличилась в 18 раз. Анализируя политические шаги Гитлера накануне и в начале Второй Мировой войны, можно допустить, что все его действия были обусловлены получением огромного фактического материала, основанного на перехвате

и дешифровке государственной и военной переписки стран, которые он планировал аннексировать или захватить.

С ноября 1940 года венгры начали перехватывать и передавать немцам радиопереговоры советских ВВС. Служба военной радиоразведки имела в своём распоряжении главные посты перехвата в Лауфе и Троенбрайтцене и посты в Мадриде, Севилье, Лоррахе, Тененлохе.

В мае 1940 года с разрешения разведывательного отдела МО Болгарии на болгарской территории под видом «метеорологических станций» были открыты 3 центра радиоперехвата «Абвера», находившиеся в оперативном подчинении разведывательного центра «Абвера» при посольстве Германии в Софии: в Софии (26 человек), в Варне (18 человек) и в Бургасе (9 человек).

По легенде название станции в Софии было «Борер», а руководил ей обер-лейтенант Гротц. Основные усилия были направлены на перехват радиопереговоров из Турции и Мальты, а также из станций в Египте, Швеции, Швейцарии и вооруженных сил США в Средиземном море.

«Chi» с самого начала войны контролировало достаточно значительный объём радиообмена противника. Так, в январе 1940 года им были перехвачены 796 британских, 460 французских, 209 турецких, 160 американских радиограмм, а в марте того же года – 1649 советских, 838 британских, 676 французских, 49 испанских, 40 польских, 40 ватиканских, 39 португальских.

Всего же в январе 1940 года армейские радиоразведчики перехватили радиограммы 27 стран. Кроме того, до 1944 года около 12% текстов радиограмм «Chi» получало из венгерских источников, в частности, от прикомандированных к подразделениям «вермахта» радиоразведывательних рот.

В октябре 1943 года «Chi» возглавил полковник Хуго Кеттлер и в следующем году осуществил его реорганизацию. Теперь оно состояло из 8 групп, из которых 1-я руководила международной службой перехвата, 2-я разрабатывала технику перехвата, 5-я занималась дешифровкой, а 6-я – перехватом телетайпного и международного радиообмена.

Собственная служба радиоперехвата была и у рейхсминистра авиации Германа Геринга – Научно-Исследовательский институт «FA» (нем. Forschungsamt) Министерства авиации, который состоял из 12 «исследовательских бюро» и огромной сети постов перехвата информации как внутри «рейха», так и за рубежом.

Для удовлетворения своих оперативных потребностей «FA» использовал 5 различных типов станций радиоперехвата,

называемых исследовательскими центрами. Станции были классифицированы по виду перехвата информации следующим образом: A – телефон, B – радиосвязь, C – радиовещание, D – телеграф, F – почта.

Станции «B», как правило, были расположены за пределами населенных пунктов, в зоне хорошего радиоприема. Радиосообщения перехватывались КВ приемниками, а затем передавались в письменном виде в штаб-квартиру «FA». Существовала только одна станция «C», которая осуществляла мониторинг радиовещания из других стран. Помимо станций, действующих в Германии, были созданы оперативные подразделения «FA» в оккупированных странах. В Нидерландах и Польше станции перехвата устанавливались наступающими войсками.

Сначала в службах радиоперехвата, шифрования и дешифровки «рейха» работало свыше 100 тысяч человек. Важнейшей причиной выдающихся успехов немецких спецслужб были исследование и уникальные разработки немецких учёных и инженеров в сфере математического анализа, приёма, передачи и обработки сигналов разной формы, частоты и мощности.

Немецкое правительство финансировало их в таких же объёмах, как и обычные системы вооружения Германии. Геринг непосредственно отвечал за развитие немецких вооружений и, естественно, не забывал о своём «FA», которое обеспечивало ему огромную власть не только в «рейхе», но и во всём мире. В дальнейшем Геринг монополизировал в Германии службу перехвата и дешифровки, для чего подчинил себе радиоразведку «Абвера».

На Восточном фронте немцы развернули сеть подчинённых штабам армий 10 радиоразведывательных рот. На каждом участке фронта длиной от 100 до 150 километров действовали до 2-х таких рот, составлявших основу немецкой системы перехвата советских сообщений. Кроме того, в состав радиорот батальонов связи каждой пехотной дивизии были включены радиоразведывательные взводы, а на особо важных участках боевых действий дополнительно размещались стационарные радиоразведывательные пункты.

Все эти подразделения вели усиленное наблюдение за советскими войсковыми радиопередатчиками, чтобы, не раскрывая факта осуществления радиоперехвата, выявлять дислокацию частей, местонахождение штабов, характер действий войск. Они также стремились вести с нашим станциями радиоигру путём перестановки в перехваченных советских радиограммах цифровых групп и повторной их передачи

в «искажённом» виде на тех же частотах.

Между тем созданная в начале 1920-х годов служба радиоперехвата и дешифровки немецких ВМС, существенно повлиявших на ход войны, оказалась немногочисленной и наименее известной среди аналогичных ей спецслужб. Командующий ВМС адмирал Дёниц называл его Службой наблюдения *«B-Dienst»* (нем. *Beobachtungdienst)*.

Она не «дружила» с коллегами из других родов войск, но её успехи были наиболее значимыми. Так, к февралю 1942 года «*B-Dienst*» достигла значимых результатов в радиоперехвате и раскрытии «конвойного шифра». Она читала большую часть зашифрованных им радиограмм, которые относились не только к североатлантическим конвоям, но и к операциям в Средиземном море и других районах мира.

К октябрю 1942 года «*B-Dienst*» читала радиообмен с конвоями союзников настолько быстро, что Дениц иногда получал информацию о будущем движении судов за 10—20 часов до фактического осуществления того или другого морского манёвра. Эта информация дополнялась перехваченным ежедневным радиообменом между командованием британского ВМФ на подходах к британским островам и канадскому Галифаксу, где был расположен штаб конвойных операций.

Хотя основные усилия «*B-Dienst*» были сосредоточены против западных союзников, не обошли они своим вниманием и Восточный фронт. До нападения на СССР, для наблюдения за районом Баренцева моря немцы использовали радиопеленгаторную станцию в норвежском городе Киркенес. Более восточные районы были вообще недоступны. Понятно, что такая ситуация немцев не устраивала.

В 1942 году на советском острове «Земля Александра» архипелага «Земля Франца-Йосифа» секретно была развёрнута 24-я база метеорологической и пеленгаторной радиослужбы «кригсмарине». Здесь находился пункт отдыха и пополнения запасов немецких подводников, а также аэродром.

Посты радиоперехвата были развёрнуты и на других секретных базах немецких подводников в советской Арктике. Советская служба радиоразведки неоднократно фиксировала сеансы связи немецких подлодок с радиостанциями, находящихся на территории СССР.

Кроме того, немцам помогали финские криптоаналитики. Так, в начале июля 1942 года финский центр радиоперехвата в Сортавала перехватил шифртелеграмму с советской авиабазы, расположенной неподалёку от Мурманска. Телеграмма была зашифрована 2-хзначным цифровым кодом, которым обычно

шифровались второстепенные сообщения.

Шифр был давно «раскрыт» финскими аналитиками, определившими, что переписка неинтересная, поэтому читали её лишь время от времени на всякий случай. Поскольку телеграмма оказалась достаточно длинной, а других телеграмм в этот день не было, то её решили дешифровать. Из-за плохой слышимости, или недостаточной квалификации радиста, получатель многократно просил её повтора, поэтому в результате фины получили идеально дешифрованный текст.

Можете представить себе удивление финских дешифровщиков, когда вместо ожидаемой несерьезной информации о доставке пайков и валенок они получили полное описание большого конвоя с военным грузом, который направлялся в СССР из Исландии.

Речь шла о караване «PQ-17». Было указано всё: его состав, названия кораблей сопровождения, точный маршрут с указанием времени отправки и прибытия в порт назначения. Фины немедленно передали эту телеграмму немцам, которые получили возможность обстоятельно подготовиться к нападению на него.

Сначала немцы попробовали использовать для перехвата конвоя большие военные корабли, в частности, тяжёлый крейсер «Тирпиц» и эсминцы сопровождения, но при выходе из базы они были обнаружены британскими ПЛ. Из-за этого немцы решили вернуть надводные корабли на базу, а удар по конвою нанести бомбардировщиками и ПЛ. В тот же день немцы узнали, что корабли сопровождения оставили конвой без прикрытия, и поэтому немецкие силы могли действовать безнаказанно.

7. Радиоконтрразведка Рейха

Военная радиоконтрразведка в Германии была создана в 1925—26 годах. Быстрое развитие технологий радиосвязи и радиоперехвата в Германии давало «Абверу» возможность не только перехватывать вражеские передачи, но также находить и уничтожать передатчики вражеских агентов. Первая задача решалась службой радиоперехвата, вторая – службой безопасности связи и радиоконтрразведкой.

Служба безопасности связи несла ответственность за радиоконтрразведку – группу «k» отдела «Абвер-III» (далее – подотдел «IIIk») под руководством капитана II ранга Шмолински. Он нашел хорошее применение радиолокационной технике, которая сделала возможным обнаружение неизвестных передатчиков средствами радиопеленгации.

И такую возможность подсказал руководству контрразведки именно ВМФ. Для флота важно было определять координаты кораблей в открытом море. Если 2 удаленные друг от друга станции с направленными антеннами могли определить азимут корабельного передатчика, то судно находилось в точке пересечения 2-х лучей. Так родилась радиоконтрразведка.

У подотдела «IIIk» появились, по крайней мере на бумаге, некоторые идеи насчет того, что будет представлять собой будущая война против вражеских радистов. По предположениям офицеров «Абвера», с помощью портативного оборудования для определения направления появится возможность засечь передачу вражеской рации и быстро определить её координаты. Конечно, такого оборудования ещё не существовало, но они были уверены, что когда-нибудь появятся специалисты, способные его создать.

Отнять у «Абвера» радиоконтрразведку попыталась Полиция охраны порядка «Orpo» (нем. Ordnungspolizei) под руководством обергруппенфюрера «SS» (нем. Schutzstaffel – отряд охраны) Курта Далюге. Закон о нелегальных передатчиках 1937 года дал полиции возможность заявить свои права на ведение радиоконтрразведки.

Полиция «Orpo» создала Управление разведывательной связи, которое возглавил оберфюрер «SS» Роберт Шлаке. В его составе было не меньше 2-х тысяч сотрудников, 7 стационарных пеленгаторных станций и несколько КВ раций. Однако глава «RSHA» (нем. Reichssicherheitshauptam – Главное управление имперской безопасности) Рейнхард Гейдрих не собирался терпеть такую концентрацию власти в руках Далюге и решился на создание собственной службы радиоперехвата.

Поэтому в сентябре 1939 года он приказал сформировать службу наблюдения за объектами, которые до сих пор находились только в ведении «Абвера», а именно за «оперативными передатчиками вражеских разведслужб». Образование радиошколы службы безопасности «SD» (нем. Sicherheitsdienst) возвестило о притязаниях Гейдриха на ведение радиоконтрразведки.

Соперничество в руководстве «SS» передавалось на более низкие уровни полицейской машины. Первоначально Гейдрих предложил, чтобы внутри «RSHA» за радиоконтрразведку отвечал III отдел (внутренняя служба безопасности). Но начальники подразделений «RSHA»: тайной государственной полиции IV отдела «Gestapo» (нем. Geheime Staatspolizei) Генрих Мюллер и VI отдела (внешняя разведка «SD») Вальтер Шелленберг вскоре начали оспаривать это решение.

Каждый из них был занят созданием собственной империи: Мюллер постоянно пытался поставить во главе этой сети своего собственного специалиста, тогда как Шелленберг заявлял о своей личной ответственности за радиоконтрразведку.

Со временем военные стали понимать, что постепенно проигрывают борьбу с силовыми структурами Германии. С началом войны место нелегальных любительских передатчиков заняли законспирированные вражеские радисты, но «Orpo» продолжала утверждать свои права на работу с ними. Все это насторожило и усилило противодействие военных.

«Вермахт» смог вовремя остановить «захват» сыщиками «SS» сферы радиоконтрразведки. Низкая эффективность радиопеленгаторов, используемых «Orpo», позволила «OKW» потребовать своего единоначалия в этой области. В конце лета 1940 года Гитлер с этим согласился, и постепенно сформировалась новая «тайная сила», которая в конце концов и обрекла на поражение советскую разведывательную сеть.

В отделе связи «вермахта» «WNV» была сформирована новая служба наблюдения из радиоспециалистов «вермахта», главным образом бывших радиолюбителей. Ее усилили энтузиастами из подразделений сухопутных войск, ВМФ и ВВС. 10 сентября 1940 года радионаблюдение возглавил подполковник Ганс Копп, опытный инженер в области связи.

За очень короткий период новая служба, которая официально стала называться Службой безопасности связи, сформировалась окончательно. Хотя ее персонал был военным, «Абверу» он не подчинялся. Удивительно, но военной контрразведке не разрешалось иметь в своем составе радиоконтрразведку, без которой противодействие советской разведке было просто

немыслимо.

Глава «Абвера» адмирал Канарис относился к нацистскому режиму критически, и его противники в структурах безопасности и полиции постарались подстраховаться, чтобы не допустить «утечки» власти в этом направлении. Его фактически заставили передать свой подотдел «IIIk» в «WNV», но разрешили сохранить подотдел «Ii», отвечавший за агентурную радиосеть и службу радиопереговоров.

Когда дело касалось «WNV», разделение полномочий на высших уровнях руководства «Вермахта» было исключительно запутанным. За 6 дней до начала войны «OKW» назначило руководителем «WNV» убежденного нациста генерала Эриха Фельгибеля. Он должен был следить и отвечать за связь между службами «OKW» и различными театрами военных действий.

В его ведении находились как вопросы связи, так и радиоразведки. Фельгибель обеспечивал бесперебойную связь между всеми государственными, партийными и высшими военными органами, руководил развитием средств связи и т. п. В руках Фельгибеля также находилась организация радиосвязи между Гитлером и Верховным Главнокомандованием, включая распределение шифров и кодов.

Будучи главой «WNV», он ещё являлся начальником службы связи Главного командования сухопутных войск «OKH» (нем. Oberkommando des Heeres) и главным уполномоченным по техническим средствам связи. Для параллельной работы в «WNV» Фельгибель использовал своего заместителя генерал-лейтенанта Фрица Тиле. Под руководством Фельгибеля тот был реальным руководителем «WNV».

«WNV» занимал прочную позицию по отношению ко всем службам связи 3-х родов войск, поскольку с технической точки зрения обладал фактической монополией внутри «вермахта». На это указывают названия его подразделений:

– сектор телекоммуникаций – поддерживал связь с почтовым ведомством и представлял пожелания военных со стороны всех 3-х родов войск;

– радиосектор – отвечал за основные радиостанции вермахта и выделял частоты для всех родов войск;

– сектор шифров «Chi» (прежний «Абвер-II») – занимался дешифровкой секретных правительственных радиограмм зарубежных стран;

– отдел общего руководства техническими средствами связи – контролировал обслуживание, распределение и замену радиооборудования.

С началом войны служба радиоконтрразведки (прежний

подотдел «IIIk») капитана II ранга Шмолински и служба радионаблюдения (служба безопасности связи) подполковника Коппа были объединены в составе отдела связи «WNV». Там они образовали 3-ю группу или, на официальном жаргоне рейха: службу «OKW/WNV/FuIII», а офицеры радиоконтрразведки переехали в офис «WNV» на Маттхайкирхплатц в Берлине.

В июне 1941 года Гитлер постановил, что «вермахт» является главным экспертом по всем вопросам радиоконтроля. Едва этот приказ был подписан, как первые радиограммы советских разведчиков бросили вызов как службе безопасности связи, так и полиции.

Первая шпионская радиограмма после начала войны была перехвачена 26 июня 1941 года около 4-х часов утра: «KLK из PTX 2606 0330 32WES N14KBV». Потом последовали 32 5-значных группы цифр, которые заканчивались подписью: «AR 50 385 KLK из PTX».

Весь этот день и следующий специалисты радиоперехвата следили за «PTX», однако так ничего и не смогли понять, кроме того, что передающая станция находилась где-то на северо-западе от германо-советской границы. Но вскоре они сделали важное открытие: кто-то отвечал «PTX».

Местонахождение этой станции не вызывало сомнений: она была рядом с Москвой. Через несколько дней в эфире заработал другой радиопередатчик, который передавал такие же 5-значные группы сигналов. И ему также ответила станция, расположенная под Москвой. Всем постам радиоперехвата в Южной Германии было приказано «держать пеленг».

В результате было установлено, что одна из станций с позывными «PTX» находится в Брюсселе, а другая – в Париже. В последующие 2 недели в эфир друг за другом выходили новые передатчики (в том числе и в Берлине), которые использовали те же 5-значные группы чисел. И всем им отвечала Москва.

В результате перехвата зашифрованных радиограмм служба перехвата начала отслеживание деятельности советских разведчиков (на жаргоне контрразведки радисты назывались «музыкантами», «пианистами», руководители и координаторы – «дирижёрами», а передатчики – «пианино»).

В эфире работало много радиопередатчиков, то есть целый «оркестр», или «капелла» по-немецки. Радиоконтрразведка определила, что «музыканты» ориентировали свои передачи на Москву, поэтому «капелла» стала «красной».

В июле 1941 года на Москву заработали еще 3 радиопередатчика из нейтральной Швейцарии, которым радиоконтрразведка дала название «Красная тройка». К этому

времени было зарегистрировано уже 78 шпионских передатчиков, а к октябрю их число возросло ещё на десяток. К июлю 1942 года на территориях, оккупированных немцами в Европе, работало 325 подпольных советских передатчиков, предположительно большинство из них на Восточном фронте.

Появление множества шпионских групп и радиостанций в 3-м Рейхе застало немецкие контрразведывательные службы врасплох. Эксперты тщетно вслушивались в радиопередачи своего противника, а радиопеленгаторы «вермахта» и полиции безрезультатно нащупывали убежища «красных» шпионов. Немцы явно столкнулись с очень сложной задачей.

Поток радиограмм демонстрировал бессилие немецких спецслужб. Станции радиоперехвата «FuIII» прилежно записывали шифрованные сообщения невидимого противника. Адресные группы цифр загадочных посланий аккуратно регистрировались в списке позывных, который вела радиоконтрразведка.

За несколько первых месяцев войны было передано в Москву несколько сотен радиограмм. Ночь за ночью и день за днём пеленгаторы абвера ловили зашифрованные 5-значные сигналы, однако немецкие дешифровальщики не могли раскрыть советский шифр.

Пеленгаторы «FuIII» были несовершенны. ВВС к тому времени располагало более мощными установками в Восточной Пруссии, Силезии, Венгрии и Румынии, но отказывалось предоставить их в распоряжение службы безопасности связи, поскольку Фельдгибель и Тиле отказывались выполнить просьбу Геринга передать в его «FA» сектор «Chi».

Поначалу радиоконтрразведка «FuIII» располагала только пеленгаторами небольшого радиуса действия, но и они могли работать только после определения района местонахождения вражеских передатчиков. К тому же эти установки имели крупные габариты, которые не позволяли подобраться к подпольному передатчику незамеченными.

«Вермахт» создал так называемый мобильный пеленгатор, но для его перевозки требовался грузовик. Кольцевую антенну метрового диаметра приходилось располагать на крыше фургона, которую заметит разведчик, контролирующий улицу во время выхода радиостанции в эфир.

Но ничего другого у немецкой контрразведки для розыска тайной сети советских передатчиков не было. Перехваченные радиограммы имели такой сложный шифр, что дешифровщики «WNV» оставили всякие попытки его раскрыть.

И все же у радиограмм было одно слабое место: попади в руки противника ключевое слово или даже сама книга, и вопрос

расшифровки становился делом времени. Именно это дешифровщики «FuIII» пытались делать в начале 1942 года, когда начали разбираться с бумагами, захваченными в конспиративной квартире советской разведки на Рю де Атребайтес.

Служба безопасности связи (радиоконтрразведка) в офисе «WNV» на Маттейкирхплац тем временем собрала группу дешифровщиков, которую возглавил человек исключительного ума доктор Вильгельм Ваук.

Он являлся одним из самых ценных специалистов «OKH/In7/VI/12». Эти иероглифы указывали на радиослужбу инспекции связи высшего армейского командования, и его только на время одолжили службе безопасности связи.

В. Ваук отобрал команду из студентов-математиков и филологов, призванных на военную службу в армейские и авиационные подразделения связи, а затем собрал их в своей новой шифровальной группе при управлении безопасности связи.

Эти молодые интеллектуалы в солдатской форме, специалисты по составлению сравнительных таблиц и вероятностным расчетам, по своей молодости и горячности не учитывали, что противник их подслушивает.

Один из сотрудников В. Ваука – капрал Хорст Хайльманн из службы связи Люфтваффе – сотрудничал с главным советским агентом Харро Шульце-Бойзеном, который и внедрил его в подразделение шифровальщиков в качестве специалиста по дешифровке английских, французских и русских радиограмм.

Среди захваченных документов оказались полусгоревшие листки, которые полицейский обнаружил в камине дома №101 на Рю де Атребайтес. Совершенно очевидно, что их бросил туда советский радист Макаров, когда пытался спастись бегством. На уцелевших клочках можно было разобрать колонки цифр.

В. Ваук сразу заподозрил, что на этих листках записана таблица кодов советской разведки, а поскольку захваченные русские агенты продолжали хранить молчание, он решил заняться ими самостоятельно.

За 6 недель дешифровщики перепробовали для разгадки шифросистемы все известные математические комбинации, но без особого успеха. Им удалось прочитать только одно слово: «Проктор». И теперь проблема состояла в том, чтобы найти этого «Проктора».

В конце концов на службу в Главное командование сухопутных войск отправился переводчик и радист Хорст Хайльманн. Его друг Харро Шульце-Бойзен ввёл его в берлинскую группу борцов Сопротивления.

Уже в 17 лет Хорст закончил учебу и поступил

в разведслужбу Люфтваффе, где стал первоклассным специалистом. Его отправили подразделение переводчиков в Мейсен. Будучи отличным математиком, он с отличием сдал там экзамены по кодам и шифрам и получил назначение в восточный сектор декодирования «FuIII», который отвечал за дешифровку советских радиограмм.

Служба безопасности связи могла проникнуть в тайну разведывательной сети только, если бы удалось обнаружить сам передатчик. Хотя КВ радиостанция сделала передачу информации быстрой и почти незаметной, тем не менее была возможность возможность найти сам передатчик.

Как только оператор начинает радиопередачу, он сразу попадает в поле зрения подразделения радиоперехвата контрразведки противника. Единственный шанс на выживание – вести передачи из какого-нибудь укромного места и как можно короче, чтобы управиться раньше, чем появятся преследователи.

Разумеется, радисты предпринимали максимум предосторожностей для защиты от пеленгаторов противника. Передатчики размещали в густонаселенных городских кварталах и труднодоступных переулках. Им приходилось часто менять свое расположение и графики выхода в эфир; их позывные постоянно менялись, использовались новые частоты.

Для предупреждения о приближении противника выставляли наблюдателей. Радисты обычно работали на верхних этажах зданий, чтобы в случае крайней необходимости в последний момент уйти по крышам.

Теоретически определение местонахождения передатчика трудности не представляет. Когда неизвестный оператор выходит в эфир, две группы наблюдателей, оснащенных пеленгаторными установками, приступают к определению направления распространения радиоволн. Оба подразделения расположены на некотором расстоянии друг от друга, и каждое из них при помощи направленной антенны определяет азимут.

Полученные данные сообщают командиру, который при помощи особых транспортиров определяет точку пересечения, в которой находится передатчик. Достаточно одного взгляда на карту, чтобы определить часть города или даже улицу, где тот работает.

Однако на практике поиску вражеского передатчика мешают почти непреодолимые препятствия. Пересечение лучей указывает его место только приблизительно. Когда наблюдатели доберутся до нужной части города, перед ними окажется нагромождение зданий, в одном из которых должна находиться рация.

Поэтому направление приходится определять заново, и тут

начинаются настоящие трудности. Появление грузовика с антенной на крыше насторожит наблюдательные посты противника, и радиопередатчик замолчит раньше, чем подразделение сможет приступить к работе.

Поскольку лучшим оборудованием располагало «FA» Геринга, Копп дал задание берлинскому взводу пеленгаторов ВВС. В качестве камуфляжа они потребовали форму связистов-ремонтников, укрыли в надежных местах на улицах свое оборудование и за работой походили на ремонтников кабельной связи.

К 21 октября 1941 года отряды пеленгаторов достигли своей цели и засекли приблизительное размещение передатчиков в Берлине. «FuIII» приказала задействовать пеленгаторы малого радиуса действия. Казалось, через несколько дней удастся точно определить дома, в которых работали передатчики.

Однако советский радист заподозрил неладное, и 22 октября берлинские передатчики внезапно замолчали. Вслед за этой неудачей в Берлине «FuIII» была вынуждена обратить особое внимание на активность передатчика с позывными «РТХ», работавшего на западе.

По расчетным данным он находился в Бельгии. Однако время поджимало, поскольку с каждым днем становилось все очевиднее, что график выхода в эфир и частоты этой рации очень схожи с берлинскими. Возможно, она могла оказаться самой главной из всех выходивших в эфир.

Радиоконтразведка обратились за помощью к «Абверу». Подотдел «IIIf», отвечавший за контрразведку против тайных служб противника, во главе с полковником Роледером мог точнее установить его координаты. После начала войны в отделе «Абвер-III» собрался самый большой штат сотрудников немецкой разведки.

Его станции слежения покрывали контрразведывательной сетью всю территорию оккупированной немцами Европы. Группа специалистов подотдела «IIIf» включилась в охоту на «РТХ», используя «сеть Адольфа» – прямую шифрованную телефонную сеть, связывавшую «Абвер» в Берлине со всеми её управлениями как в рейхе, так и на оккупированной территории.

Наконец персонал КВ станции радионаблюдения «Запад» запеленговал шпионскую рацию в Брюсселе. «FuIII» сразу откомандировала туда капитана Хуберта Фрайера, который командовал радиоротой штаба оперативного руководства «OKW», с подразделением опытных операторов и новым пеленгаторным оборудованием.

Фрайер привез с собой новый КВ пеленгатор, который вместе

со встроенной антенной помещался в обычном чемодане. От чемодана к уху оператора тянулся тонкий провод. Больше не нужен был грузовик с «предательской» антенной на крыше, предупреждавшей о приближении контрразведчиков, и никакого звука мотора.

Люди Фрайера приступили к работе, и через 2 недели установили расположение первого передатчика «Красной капеллы». 13 декабря 1941 года отряд солдат бесшумно поднялся на второй этаж дома 101 на Рю де Атребайтес в Брюсселе. Они ворвались в одну из комнат и арестовали там русского радиста Михаила Макарова и шифровальщицу Софью Познанскую.

В июле 1942 года советская разведка в Западной Европе потеряла всю свою мощь, когда в Брюсселе немцы схватили главного радиста «Красной капеллы» Иоганна Венцеля. Потеря Венцеля с его рацией лишила бельгийскую сеть её центральной фигуры – основного радиоспециалиста.

В конце августа 1942 года Хорст по службе получил перехваченное и расшифрованное советское сообщение с адресами агентов, и сразу же попытался связаться по телефону с Шульце-Бойзеном. Но в скором времени более, чем 120 членов движения сопротивления были арестованы.

Немецкие спецслужбы разрушали опорные пункты «Красной капеллы» один за другим. «Gestapo» уничтожило всю берлинскую группу – лучший источник информации. Еще до этих событий арест немцами радистов супругов Сокол нанес серьезный ущерб французской сети советской разведывательной группы Леопольда Треппера.

После захвата берлинского передатчика «Красной капеллы» криминальный комиссар Томас Амплетцер, специалист по «радиоиграм» подотдела «IVA2» «Gestapo», тут же распорядился о подготовке «контригры» с Москвой.

«Радиоигра» была любимым методом немецкой контрразведки. Инструкции требовали, чтобы любой вражеский тайный передатчик, который будет захвачен вместе с обслугой, немедленно начинали использовать против прежних хозяев. Это преследовало 2 цели: получить полную картину вражеской разведывательной деятельности в собственном лагере и запутать противника, снабжая его дезинформацией.

В «Абвере» этим занимался подотдел «IIId» под руководством полковника резерва доктора Шефера. Он осуществлял подготовку материалов для «игры» с агентурой противника и «радиоигры» для агентов подотдела «IIIf».

Амплетцеру в организации «радиоигры» помогал советский радист Йоган Венцель, главный радист «Красной капеллы»

в Западной Европе, арестованный в июне 1942 года. Он уже сослужил «Gestapo» неплохую службу, сыграв главную роль в охоте за советскими агентами в Бельгии и дешифровке службой «FuIII» перехваченных радиограмм.

Венцель выдал своим новым хозяевам ключи к русским шифрам, и Амплетцер вскоре установил радиосвязь с советским разведцентром. Сразу после ратрома шпионской сети в Бельгии и Голландии Амплецер в Берлине приказал начать радиоигру с Москвой с использованием захваченных передатчиков.

4 рации включились в радиоигру: операция «Айхе» (дуб) с использованием передатчика советского радиста Сезе, операция «Танне» (ель) – Винтеринка, «Вайде» (ива) – Венцеля и «Бухе-Паскаль» (бук) – Райхмана. С арестом радистов Треппера во Франции появились ещё 2 передатчика, которые положили начало радиоопераций «Эйфель I» и «Эйфель II».

Впоследствии их объединили под кодовым названием «Марс-Айфель». «Марс» в данном случае означал Марсель, поскольку немцы хотели поддержать легенду, что советский агент «Кент» по-прежнему ведет радиопередачи из этого города.

Амплетцер начал управлять своим фальшивым «оркестром» в ноябре 1942 года. Радиосвязь быстро удалось наладить, и вскоре обмен сообщениями между Москвой и Западной Европой пошел так же гладко, словно и не прерывался. У Центра подозрений, похоже, не возникло, а задержку с выходом в эфир «Gestapo» объяснило техническими неполадками.

Немцам очень хотелось передать радиосвязь в руки перевербованных агентов «Красной капеллы». Конечно, приходилось опасаться, что в любой момент невольные помощники могут предупредить советский разведцентр при помощи какого-нибудь заранее согласованного сигнала. Единственная ошибка в определенной группе цифр или позывных могла положить конец тщательно спланированной «радиоигре».

Поэтому «Gestapo» не позволяло никому из бывших агентов даже прикасаться к настоящим передатчикам. Перевербованные радисты работали на учебных ключах, а их сообщения записывались на магнитную ленту. Таким образом немцы могли изучать, а затем имитировать «почерк» каждого радиста.

После долгих тренировок по копированию «почерка» бывших противников немецкие радисты передавали тщательно подготовленную информацию в Москву. Перевербованным радистам приходилось постоянно присутствовать во время приема и передачи радиограмм, поскольку московское начальство могло внезапно вклиниться в передачу и потребовать сообщить заранее условленный пароль.

В процессе радиоигры сначала передавались только такие сведения, которые противник был не в состоянии проверить. Подобного материала оказалось явно недостаточно, поэтому в материалах радиоигры стали преобладать подлинные данные. Это условие выросло в большую проблему.

Москва требовала главным образом военную информацию, но передавать её противнику надо было без ущерба для безопасности собственных войск. Для контрразведки этот вопрос был самым болезненным, ведь она зависела от доброй воли руководства «вермахта», без санкции которого никакой военной информации получить было невозможно.

Когда Москва запрашивала у своих агентов военные сведения, «специальному отряду» Амплетцера приходилось запрашивать их у французского отделения «Абвера» в Париже. В свою очередь, «Абвер» обращался за одобрением к главнокомандующему группой армий «Запад» и после его получения составлял необходимую сводку, которая шифровалась и отправлялась в Москву.

Однако, несмотря на все бюрократические препоны, Амплетцер со своими специалистами в Париже ухитрялись отвечать на запросы советского Центра достаточно быстро. Поток информации между Разведцентром и «Gestapo» рос с каждой неделей. Москва не усомнилась в своих агентах на Западе, и ее запросы становились все более конкретными и настойчивыми.

Чем подробнее становились вопросы Москвы, тем больше она вынуждена была выдавать все ещё работавшую на Западе сеть своих информаторов, а именно это и было целью «Gestapo». Там имели все основания полагать, что советская разведсеть во Франции, Бельгии и Голландии разрушена, но ещё оставалась сеть Коминтерна и подполье французской компартии, которых также подключили к сбору информации.

Гораздо более важной целью была советская разведсеть под руководством Шандора Радо в Швейцарии. После разгрома других групп на неё возложили ответственность за обеспечение Москвы информацией с самых высоких уровней руководства «вермахта». Радо занимался только перехватом информации по каналам швейцарской армейской спецслужбы, у которой оказались замечательные связи в ставке фюрера.

Следующей целью «Gestapo» стало заставить Москву выдать последних оставшихся на Западе агентов. Одну победу «специальный отряд» записал на свой счет, когда удалось убедить советский Разведцентр сообщить местонахождение одного из подпольных передатчиков французских коммунистов, который немцы немедленно захватили.

Когда передатчик «Кента» вышел из строя, «Gestapo» попросило Москву обеспечить надежного радиотехника из французской компартии. Центр сразу порекомендовал для этой цели товарища Жожо, который собирал для своей партии КВ передатчики. Его арестовали, и он выдал известных ему информаторов, которые вскоре оказались в тюрьме.

5 июня 1943 года главнокомандующий группой армий «Запад» в письменной форме изложил свои соображения против передачи разведданных для продолжения «радиоигры» «Эйфель». Он отметил, что московский Центр вот уже некоторое время ставит настолько конкретные вопросы военного характера, что «радиоигра» может продолжаться лишь в том случае, если на них будут даваться столь же конкретные ответы, «иначе Москва поймет, что ее водят за нос».

Поэтому он решил не брать на себя ответственность за предоставление информации, необходимой для «радиоигры». Он также придерживался того мнения, что военное положение немецких войск на Западе таково, что нет никакого смысла вводить Москву в заблуждение.

Однако, по мнению контрразведчиков, смысл продолжать игру все-таки был. Служба безопасности «SD» (нем. SicherheitsDienst) и Полиция безопасности «SiPo» (нем. Sicherheitspolizei) были соответствующим образом проинформированы. Что из этого получилось, не известно, однако 17 июля 1943 года главнокомандующий группой армий «Запад» предоставил немецким контрразведчикам дополнительный материал для продолжения игры.

После бегства Треппера в сентябре 1943 года отделение «Абвера» во Франции положило конец «радиоигре»: «Получение дезинформационных материалов от главнокомандующего группой армий „Запад“ столкнулось со значительными трудностями, поскольку главнокомандующий придерживается мнения, что противник в Москве уже заподозрил обман… Главнокомандующий не может обеспечивать необходимой информацией для ответов Москве также по чисто военным причинам».

В «RSHA» также пришли к выводу об окончании операции, поскольку организации «Красной капеллы» во Франции и Бельгии давно ушли в историю. После этого началась «радиоигра» «Кента» (операция «Марс»), продолжавшаяся до конца войны. Также продолжалась операция по внедрению агентов во французское подполье, но «радиоигра» «Красной капеллы» постепенно завершалась.

8. Радиоигры «Абвера» с «MI6»

Кульминацией деятельности немецкой радиоконтрразведки «Абвера» во время Второй Мировой войны стали две «радиоигры», проведенные против британской разведки «MI6». Они получили от задействованных немецких спецслужб следующие названия: акция «Nordpol» (нем. северный полюс) и дело «Porto II».

Акция «Nordpol» началась в августе 1941 года, когда начальником отделения «IIIf» в Нидерландах был назначен майор Германн Гискес, работавший до этого в парижском центре «Абвера». Перед ним была поставлена задача выявить те связи с Лондоном, которые использовались вражескими агентами в Голландии. Уже вскоре в голландское подполье были внедрены немецкие информаторы.

В конце ноября Гискес получил данные о деятельности группы британских агентов в Гааге. Они держали радиосвязь с британским разведцентром в Лондоне, и при передаче донесений у них был позывной «RLS». С помощью службы радионаблюдения удалось точно определить технические параметры радиопередач: время сеансов, основные частоты и порядок их изменения, продолжительность сеансов связи и т. д.

За передатчиком «RLS» теперь стали постоянно следить. Гискес придавал значение тому, чтобы выявить почерк и все особенности радиста, направляющего с передатчика сообщения в Лондон. Сначала надо было захватить эту группу и ее передатчик, а затем начать «радиоигру».

Этой задаче было подчинено все, потому что план Гискеса обещал успех. Уверенность в этом усиливалась еще и потому, что «Абверу» удалось внедрить в группу своего агента. Обстоятельства складывались в его пользу, поскольку у вражеской разведки в Нидерландах было явно немного агентов, с помощью которых она захотела бы начать строить разведсеть.

Но важнейшими предпосылками для успешной долгосрочной контригры был арест до последнего человека всех лиц, связанных с работой вражеского передатчика «RLS» в Нидерландах. Ни один из входивших в эту сеть агентов не должен был «улизнуть» и передать в Великобританию донесение об аресте группы.

Наконец 6 марта 1942 года был предпринят захват группы. «Абверу» стало известно точное местонахождение передатчика «RLS», и он провел необходимую подготовку для арестов. В тот же день удалось арестовать 4-х агентов, входивших в шпионскую группу.

Вражеский радист, обслуживавший эту радиостанцию,

оказался нидерландским гражданином и британским лейтенантом по фамилии Лоуэрс. Через него в немецкие руки попали секретные шифры, которые он использовал для шифрования и дешифровки шпионских радиограмм.

Поскольку этот радиообмен между Лоуэрсом и британским Центром в последние месяцы контролировался службой радиоперехвата «Абвера» и записывался, теперь с помощью шифров стала возможной дешифровка всех перехваченных радиограмм.

Это означало, что подполковник Гискес сразу смог составить ясную картину того, какие задачи «MI6» ставила перед группой с позывным «RLS» и что арестованные британские агенты уже успели сделать.

Поэтому было относительно легко вычислить, какие дальнейшие действия предприняли бы агенты группы Лоуэрса, если бы оставались на свободе. Далее уже было не особенно сложно проинструктировать своих доверенных лиц таким образом, словно они и выполняли задачи, поставленные шпионской сетью «RLS».

Группа должна была подыскивать и готовить в Голландии места для сброса оружия с воздуха, а также снаряжения для диверсионных актов и для работы агентов. Ставилась также задача вербовки лиц, пригодных для дальнейшего использования в качестве агентов и сотрудников.

Чтобы лишить Лондон всяческих подозрений, следовало прежде всего сохранить непрерывность радиопереговоров, для чего нужно было добиться согласия захваченного радиста. Его «почерк» при передаче радиограмм был в Лондоне, конечно, хорошо известен, и, если бы его кем-то подменили, это сразу стало бы известно.

Каждый радист обладает ему одному присущим «почерком», характерными особенностями, с которыми он нажимает на клавиши радиостанции, и определенной скоростью при передаче радиосигналов. Различие очень тонкое, но опытные радисты, которые долгое время поддерживали взаимный радиообмен, узнают друг друга по характерным особенностям. Они распознают радиосигналы словно почерк.

Радист Лоуэрс согласился сотрудничать с немцами, и с середины марта отделение «IIIf» в Голландии начало «радиоигру» с Лондоном, используя передатчик «RLS». Она быстро дала желаемые результаты: британцы продолжили выброску материалов и агентов.

Однако уже в апреле стало ясно, что британский центр спецопераций «SOE» (англ. Special operations executive) проводил

другие такие же мероприятия в Голландии, но уже избегал группу «RLS». Гискесу это предрекало скорый «крах» операции, но ему повезло.

Благодаря своей находчивости и удачному стечению обстоятельств он получил в свои руки все нити, с помощью которых Лондон руководил своими агентами в Голландии. Поскольку британцы сбросили 3 пары агентов, которые приземлились неудачно, они поручили группе «RLS» связаться с ними.

В результате Гискес получил много дополнительных материалов, а к концу мая 1942 года имел уже 3 самостоятельно действовавших канала связи с Лондоном и несколько условленных мест выброски. Вскоре был пойман агент Джемброуз, имевший при себе детальные планы диверсий совместно с голландской подпольной организацией (нем. Ordnungdienst – служба порядка).

Летом 1942 года акция «Нордпол» шла полным ходом. В первый раз уже в конце марта из Лондона по радио пришло поручение подобрать подходящую площадку, чтобы группа «RLS» приняла крупную партию диверсионных материалов. Одновременно сообщалось, что при этой выгрузке будет сброшен и один парашютист для усиления группы.

Подходящее место быстро нашлось. Лондон заявил, что одобряет выбранную площадку, и сразу обозначил сроки, в которые следует ждать самолет. За этой выброской последовали и другие, обеспечивающие прибытие и других агентов. Поскольку о них заблаговременно извещали, то «приемная комиссия» могла вести их планомерный прием.

Самым важным из этих агентов был нидерландец Ямбрус, прибывший в конце июня 1942 года. Как лейтенант «MI6» он имел конспиративное имя Юргенс. Для Лоуэрса он привез оперативный план с инструкциями по созданию и использованию крупной подпольной организации в Нидерландах. Однако этот план находился у агента только в голове.

Гискесу удалось разузнать об инструкциях, которые Юргенс должен был передать Лоуэрсу. «MI6» задумывала создать в Голландии многочисленную подпольную организацию, чтобы с ее помощью в нужное время нарушать или вообще перерезать коммуникации, идущие из рейха через Нидерланды в Бельгию и Францию.

После того, как Гискес ознакомился с оперативным планом «MI6», он стал целенаправленно работать над тем, чтобы в Лондоне создалось впечатление, что Лоуэрс и его товарищи осторожно и упорно работали над выполнением поставленных

перед ними задач.

Он отправил в Лондон несколько радиограмм, в которых сообщал, что группе с позывным «RLS» то в одном, то в другом голландском городе удалось завербовать новых информаторов, готовых к решительным действиям против Германии.

Целью этого радиообмена было не только вытянуть из Великобритании дальнейшие посылки с оружием и диверсионным материалом. Гискес хотел добиться того, чтобы «MI6» доверила группе Лоуэрса руководство формированием всей сети подпольных организаций в Нидерландах.

Если бы это удалось, «Абвер» мог попытаться вместо 17 сотен членов нидерландского подполья, формирование которых предусматривала британская разведка, создать фиктивные организации и провести отвлекающий маневр с долгосрочной перспективой и на широком оперативном просторе.

«MI6» поначалу не планировала ставить Лоуэрсу столь глобальных задач. Она, напротив, собиралась независимо от группы «RLS» создать другие агентурные группы, которые по отдельности занялись формированием подпольных сотен. С этой целью «MI6» на самолете забросила в Нидерланды еще 3 пары агентов-парашютистов с позывным «RLS», не оповещая об этом группу.

Однако, благодаря счастливой случайности, у подполковника Гискеса оказались в руках все нити, ведшие из Лондона к агентам, неизвестным группе RLS. Умелым использованием представившихся ему возможностей он добился того, что «MI6» перенесла все создание подпольного движения в Нидерландах на агентов группы «RLS», которые находились в его руках.

До ноября 1942 года было перехвачено еще 17 агентов, из них 5 радистов с рациями и рабочими частотами. К концу года немецкая радиоконтрразведка «доложила» Лондону, что «Ordnungdienst» уже насчитывает 17 сотен активистов, которые якобы проходят подготовку, и потому им срочно требуется одежда, белье, обувь, чай, табак, велосипедные шины и т. п.

Груз общим весом до 5 тонн не заставил себя долго ждать. С января по апрель 1943 года в места, подсказанные Лондону, спрыгнуло еще 17 агентов – прямо в руки «приемной комиссии». Они имели еще 7 независимых каналов связи.

Перед Гискесом встала проблема передавать Лондону по 14 каналам связи информацию о деятельности целых 50 агентов. Обеспечить такой объем работы его 6 перевербованных радистов не могли. Тогда он предложил Лондону «ради безопасности» законсервировать несколько раций, и с ним согласились.

В период наиболее активной фазы этой «радиоигры» (март 1942 – ноябрь 1943) противнику внушали присутствие в Голландии исключительно боеспособной организации террористов. И это побудило Лондон и его тайные службы усилить эту организацию. Было произведено около 200 выбросок, в ходе которых немецкие истребители сбили 12 британских бомбардировщиков после сброса ими материалов и агентов.

Можно себе представить, какого труда стоило немецкой стороне, чтобы 2 года подряд в таких масштабах «водить за нос» «MI6». 200 раз приходилось подбирать подходящих людей в «приемную комиссию» и своевременно отправлять их. В некоторые ночи выбросски проводились одновременно в 2-х или 3-х, иногда даже 4—5 точках.

«Приемные комиссии» должны были быть всегда пунктуальными и работать неприметно. При выдвижении к месту выброски и во время нахождения на нем, а также при возвращении следовало действовать так, чтобы не вызвать подозрение пилотов или насторожить местное население.

Каждому приему снаряжения или агентов предшествовала «радиоигра» с Лондоном. С немецкой стороны радиосвязь обеспечивали, в основном, сотрудники радиоперехвата «Абвера». Но наибольшую роль при этом играло не столько техническое развитие, сколько составление точного текста радиограмм, направляемых в лондонский Центр.

В целом за время проведения акции «Нордпол» от противника было заброшено 54 агента частично на парашютах, частично тайно переброшено по морю и высажено на побережье Нидерландов. Все они, обученные в Великобритании для проведения спецопераций, попали в руки абвера.

В плен попали 54 хорошо обученных агента. Было захвачено 15 тонн взрывчатки и различных средств для диверсий, около 3000 автоматов, 5000 пистолетов, 300 легких пулеметов, 2000 гранат, 75 раций и до 500 тысяч патронов. Кроме того, через Испанию и Швейцарию были получены огромные денежные средства в валюте этих стран для «организации курьерской связи» в Брюссель и Париж.

Были также переданы адреса явок и опорных пунктов в районах Парижа и Брюсселя. Эти адреса «Абвер» взял под наблюдение, поскольку поступающая из Лондона обширная информация могла оказаться еще более ценной, если эти пункты не будут уничтожены. Чтобы избежать подозрений у Лондона, Гискес сфабриковал убедительные доказательства действенности голландского «Сопротивления».

Он сумел переправить обходными путями нескольких

летчиков со сбитых британских самолетов в Испанию, а перед этим сообщил в Лондон по радио имена и звания этих летчиков. Показания этих летчиков после возвращения на родину однозначно доказывали, что в Голландии «все в порядке».

К тому же «Абвер» организовал и провел на судах и железных дорогах в Голландии реальные взрывы и диверсии, которые, конечно, тяжелого ущерба не причинили. Сообщения об этих «акциях» фабриковались «Абвером» и подбрасывались Лондону через иностранную прессу, главным образом – швейцарскую и шведскую.

В конце августа 1943 года 2 британских агента сбежали из плохо охраняемой полицией тюрьмы. Был развернут широкий поиск, но успеха он не дал. Стало ясно, что «радиоигра» немецкой контрразведки может быстро закончиться, как только лондонский центр получит сообщение беглецов. На всякий случай Гискес отправил в Лондон радиограмму, в которой утверждал, что беглецы являются предателями.

Но он понимал, что это ненадолго «оттянет» конец. И действительно, уже в начале декабря радиограммы из Лондона стали краткими и почти бессодержательными. Тогда Гискес запросил у Берлина разрешение прекратить эту вначале столь успешную «радиоигру», превратившуюся теперь в фарс.

Он послал голландскому отделу «SOE» прощальную радиограмму такого содержания: «Как нам стало известно, Вы с некоторого времени пытаетесь вести свои дела в Голландии без нашего участия. Мы сожалеем об этом тем более, что мы здесь, в Нидерландах, столь долго работали в качестве Ваших единственных представителей и, кажется, к обоюдному удовлетворению.

Однако можете быть уверены в том, что, если Вы замыслите нанести нам здесь, на материке, еще более масштабный визит, мы уделим Вашим представителям такое же внимание и окажем столь же радушный прием, как и прежним». Этот текст был передан открытым текстом 10-ю радиостанциями 1 апреля 1944 года, когда Гискес еще распоряжался ими. На том и завершилась акция «Nordpol».

Успех операции заключался в том, что намерения разведки противника создать обширную диверсионную группу были нейтрализованы в ходе многолетней дезинформации. Еще в начале 1944 года «MI6» верила, что в ее распоряжении в Нидерландах имеются тысячи хорошо оснащенных бойцов «Сопротивления». В действительности же сил, на которые она рассчитывала, вообще не существовало.

Кроме того, для германского военного командования

и «Абвера» многочисленные указания, которые «MI6» в сотнях радиограмм направляла прямиком немецкому радисту в полной уверенности, что она находится на связи с членами подпольной организации, были ценны и крайне содержательны.

После войны государственные комиссии Великобритании и Нидерландов глубочайшим образом анализировали операцию «Nordpol», пытаясь понять, как могла случиться подобная неудача у такой опытной спецслужбы «SOE». В результате был сделан вывод, что всему виной была определенная беспечность со стороны «SOE». Никто не додумался хотя бы однажды отправить в Голландию своих людей для контроля ситуации.

Дело «Порто II» – еще одна «радиоигра» «Абвера» летом 1942 года во Франции, когда акция «Нордпол» была еще в полном разгаре. Эта «контригра» с немецкой стороны велась иначе, нежели акция «Нордпол», и преследовала иные цели.

Военное командование иногда высказывало желание о «контригре», чтобы иметь возможность быстро и надежно передавать вражеской разведке дезинформацию о собственных военных делах, таких, как передислокация частей, маршевые колонны и перевозки. Та, конечно, и не должна была подозревать, что донесения засылаются «Абвером».

По этой причине «Абвер» «подсадил» 2-х постоянно проживавших в Париже молодых людей британской резидентуре «MI6» в Португалии, известной «Абверу» еще по делу «Порто I». Оба были доверенными лицами, действовавшими под псевдонимами Макс и Мориц, заранее прошедшими проверку на лояльность.

Согласно легенды они заявили в британской резидентуре, что имели возможность во Франции с помощью друзей заниматься шпионажем против Германии. Кроме того, они будто бы могли передавать по радио донесения в Лондон, если им дадут рацию. Один из них был радиолюбителем и правдоподобно рассказал, как им стал. В результате британцы снабдили их рацией и шифрами, и «радиоигра» началась.

С немецкой стороны имелся следующий план: Макс и Мориц согласно своей роли сразу заявили представителям «MI6» в Португалии, что они со всей осторожностью приступят к делу и сначала хотят занять в нем только своих преданных друзей.

Поэтому они, в особенности в первые месяцы, не могли передавать очень много донесений, словно им приходилось прикладывать много усилий, чтобы разузнавать самое важное. Представители «MI6» сочли это само собой разумеющимся.

Оба доверенных лица получали лишь ограниченную, но достоверную информацию для передачи в Лондон. Правда,

уходившие в Лондон донесения тщательно подбирались и формулировались по согласованию с отделением «1с» главного командования группы армий «Запад».

План «Абвера» основывался на том, чтобы постоянной поставкой точной, хотя и не очень важной информации создать у «MI6» впечатление, что Макс и Мориц для них надежны, однако неопытны и необучены. Поэтому ожидалось, что «MI6» начнет давать им неоднократные советы, указания и рекомендации, что и было целью «Абвера». Поскольку в дальнейшем «MI6» стала бы «заглатывать» дезинформацию как истину.

Для создания «игрового» материала донесений, которые отправлялись по радио в Лондон, «Абвер» поступал следующим образом. Макс и Мориц в сопровождении офицера отделения «IIIf» осматривали военные объекты, о которых было разрешено сообщать. Оба доверенных лица таким образом могли составлять сообщения на основе собственных наблюдений и формулировать собственными словами.

Затем их тексты проверялись в отделении «1с» главного командования группы армий «Запад». Исключения делались лишь в том случае, если содержание радиограмм не содержало секретных сведений.

«MI6» в первые месяцы реагировала на получаемые радиограммы, как на то и надеялся «Абвер». Лондон дал Максу и Морицу множество поручений и сообщил им, какими объектами интересуется, а какими – нет. Затем время от времени они получали директивы, как им следует постараться дополнить отдельные донесения.

По этой реакции противника можно было сделать разные выводы. Среди прочего было ясно, что разнообразные военные объекты, о которых шли донесения в Лондон, не интересовали «MI6». Но по поручениям, получаемым Максом и Морицем из Лондона, было понятно, что «MI6» особенно интересовалась определенными военными сооружениями и ведомствами. В результате были приняты дополнительные меры безопасности по охране военных тайн на этих объектах.

Успех «радиоигры» проявился в том, что вражеская разведка уже в первые месяцы прониклась к Максу и Морицу полным доверием. Так, когда они отправляли радиограммы в Лондон, в которых запрашивались личное огнестрельное оружие, снаряжение и одежда для вновь привлеченных друзей, очень быстро пришел ответ, что требуемые вещи в скором времени будут присланы.

Несколько дней спустя пришла радиограмма, содержащая точные данные, куда и когда будет поставлено требуемое

снаряжение и какие опознавательные знаки следует подавать карманными фонариками британским самолетам.

Площадка в 60—70 километрах к югу от Парижа была точно обозначена «MI6». Предположительно она там уже проводила выброски для членов движения «Сопротивления». В назначенный час Макс и Мориц отправились в указанную точку в сопровождении нескольких офицеров «Абвера». Выбранная площадка располагалась в необитаемом лесном массиве.

Точно в указанное Лондоном время послышался гул приближающегося самолета, которому фонариками были поданы условные сигналы. И вот самолет на высоте около 200—300 метров сбросил контейнеры, которые снижались, раскачиваясь на парашютах. В них помимо заказанного снаряжения были еще сигареты, продукты, деликатесы, а также изрядная сумма денег.

Эта местность для выброски в окрестностях Фонтенбло еще несколько раз использовалась летом 1942 года. Время от времени Макс и Мориц сообщали в Лондон, будто к их группе примкнули новые бойцы и им требовалось дополнительное снаряжение. Лондон незамедлительно сбрасывал заказанное.

Ожидание на месте выброски для людей из «приемной комиссии» каждый раз заставляло их переживать. С огромным напряжением ожидали даты, на которую был назначен прилет самолета. Однако все проходило хорошо. Но чем больше и продуктивнее представлялась «MI6»мнимая шпионская группа Макса и Морица, тем больше становились требования к ней.

«MI6» уже не удовлетворяли донесения, подготовленные «Абвером» по согласованию с главнокомандующим группой армий «Запад». Чем дольше продолжалась «радиоигра», тем чаще приходили Максу и Морицу требования из Лондона точнее и основательнее разведывать ход военных процессов и состояние объектов.

Но главнокомандующий группой армий «Запад» не мог решиться передать подробные данные о секретных военных объектах, которые требовала британская разведка. Сведения о противнике и его замыслах, получаемые в результате ведения «радиоигры», за такую цену ему были не нужны.

«Абверу» стало ясно, что проведение операции «Порто II» подошло к критической точке. Поскольку ценная информация не могла быть передана в Лондон, уже в ближайшие недели это приведет к тому, что из Лондона поступят радиограммы с недовлетворенной оценкой работы Макса и Морица. У «Абвера» создалось впечатление, что в Лондоне уже появилось подозрение против этих агентов.

Во Франции дела обстояли совсем иначе, нежели в Нидерландах. Британская разведка последние 2 года провела с пользой и была настолько хорошо информирована о немецких вооруженных силах, что не могла долго терпеть примитивные донесения Макса и Морица.

На такой стадии «радиоигры» прояснилось, что важнейшая цель, которую «Абвер» ставил вначале, а именно дезинформация вражеской разведки по важным военным процессам с немецкой стороны, вряд ли будет достигнута. Если «MI6» осенью 1942 года не доверяла Максу и Морицу важной шпионской работы или даже подозревала их, то было бы ошибкой пытаться навязывать через них эффективную дезинформацию.

Потому «Абвер» решил закончить «радиоигру». Это сделали таким образом, чтобы «MI6» решила, будто они были ликвидированы немецкой контрразведкой. Еще несколько недель Лондон по радио вызывал Макса и Морица. Но они больше не «откликались».

9. Радиоразведка Германии

После Второй Мировой войны Германия была разделена на два отдельных государства: Федеральная Республика Германии – ФРГ (под контролем США) и Германская Демократическая Республика – ГДР (под контролем СССР), которые создали собственные службы радиоразведки в составе министерств обороны и государственной безопасности.

В апреле 1950 года в ГДР была создано Министерство государственной безопасности (нем. Ministerium fur Staatssicherheit), сокращённо – «Штази» (нем. Stasi). Радиоконтрразведкой в нем занимался отдел «F».

За радиоперехват, дешифровку и контроль телефонных переговоров с зарубежными абонентами отвечал 3-й главный отдел МГБ, который был одним из основных заказчиков радиоприемной и звукозаписывающей аппаратуры. 270 стационарных постов радиоперехвата «Stasi» располагались в округах вдоль границы с ФРГ и в официальных зарубежных представительствах ГДР.

По данным бывших сотрудников контрразведки МГБ между 1977 и 1986 годами почти 50% всех первоначальных «наводок» на западных шпионов в ГДР получало от неофициальных сотрудников и с использованием средств и методов из так называемой «оперативной области», т. е. в ФРГ. Чуть больше 20% приходилось на сведения, полученные с использованием радиоперехвата и дешифровки криптограмм в самой ГДР.

В 1955 году в ФРГ была создана Федеральная разведывательная служба «BND» (нем. Bundesnachrichtendienstes), которая обеспечивала получение информации с каналов связи с помощью технических средств, а раскрытие шифров было возложено на её 2-й отдел (техническая разведка), в котором сейчас работают 1,5 тысячи сотрудников.

Техническая разведка по своим задачам и методам похожа на Дирекцию науки и техники ЦРУ, насчитывающий около 5 тысяч сотрудников и занимающийся операциями радиоразведки.

7 июня 1955 года были созданы Вооружённые силы Германии, или Бундесвер (нем. Bundeswehr), где контрразведывательные функции были возложены на службу безопасности Бундесвера «ASBw» (нем. Amt für Sicherheit der Bundeswehr), но права ведения военной разведки у нее нет. Поэтому политическая, военная, научно-техническая и экономическая разведка в ФРГ были сконцентрированы

в «BND», что позволило избежать противоречий между различными ответственными за это институтами.

С 1984 года служба безопасности Бундесвера «ASBw» была реорганизована в службу военной контрразведки «MAD» (нем. Amt für den militärischen Abschirmdienst). Радиоэфир морского побережья Германии контролируется радиоразведкой ВМФ. Эфир остальной части Германии контролируется Центром радиомониторинга Бундесвера «AFMBw» (нем. Amtfiir Funkiiberwachungder Bundeswehr) и «BND».

Служба «G-2/A-2» Бундесвера – один из 4-х классических отделов штабного звена. Наряду с кадровым, оперативным и боевой подготовки и отделом тылового обеспечения и снабжения она отвечала за сбор, обработку и анализ военного положения противника, однако не вела активного шпионажа. Зато эта служба с успехом пользовалась данными РЭР, собранными спецслужбами Бундесвера, которые занимались радиоперехватом и дешифровкой радиограмм войск стран Организации Варшавского договора.

Строительство Берлинской стены (1961—89) протяжённостью 155 километров заставило «BND» предпринять новые шаги для продолжения ведения разведки за советскими гарнизонами и воинскими частями в ГДР. Однако из-за того, что постоянно увеличивающиеся потери старых агентов нельзя было мгновенно восполнять новыми источниками, была сделана большая ставка на радиразведку. Техническая разведка позволяла избежать риска ареста агентов или пропагандисткой шумихи вокруг неудач «BND».

На границе с ГДР и Чехословакией был построен ряд пунктов радиоперехвата для прослушки линий коммуникаций. «BND» провела успешную операцию по перехвату канала связи командования Группы советских войск в Германии. Благодаря своим информационным возможностям «BND» смогла предсказать ввод советских войск в Чехословакию и дату начала арабо-израильской войны 1967 года.

Но с другой стороны, технические виды разведки, несмотря на свою полезность в плане «профилактической» защиты источников агентурной разведки, обладали и существенными недостатками. Огромные потоки радиоперехвата при отсутствии критериев разделения на важное и маловажное, к сожалению, не давали требуемых результатов.

Самыми актуальными в информационном потоке «BND» были так называемые «ВМ» -донесения – результаты радиоперехвата. Поэтому легче всего западногерманской разведке удавалось идентифицировать те воинские части, которые проявляли

активность в эфире, например подразделения радиоэлектронной борьбы. В принципе, части и подразделения войск связи, радиолокационные подразделения, а также подразделения ВВС являлись более легкой целью для радиоразведки «BND», чем сухопутные войска.

Проникая в радиосвязь и обрабатывая радиолокационные данные советских авиачастей, западногерманская разведка могла сделать выводы о методах летной подготовки, об уровне обучения летчиков, часах и задачах полетов, выполнении заданий и зависимости от метеоусловий. Наблюдатели на местах, конечно, не могли бы получить такие знания.

Особо хорошие знания о советских ВВС и тем самым более простое и легкое использование методов радиоразведки по сравнению с агентурной разведкой подтверждаются и годовым итоговым отчетом «BND» за 1975 год. В нем детально описывалось перевооружение с самолетов второго на самолеты третьего поколения в советских авиаполках 16-й Воздушной армии в ГДР.

Доклад свидетельствовали о хорошей информированности о войсках ПВО СССР, о сухопутной ПВО в Группах войск в странах Организации Варшавского договора, об организации системы связи и наведения истребителей-перехватчиков. Незаурядная глубина и детальность доклада объяснялись исключительно использованием различных электронных средств разведки. Потому следующие 10 лет ВВС и ПВО занимали основное место в западной разведке – и не только из-за их боевого значения, но и по причине большей доступности для радиоразведки.

В 1970-х годах благодаря дешифровке службой радиоперехвата шпионских радиограмм из берлинского радиоцентра МГБ ГДР был выявлен и арестован разведчик ГДР Гюнтер Гийом, внедрённый в ведомство канцлера ФРГ. Это разоблачение стало началом получившего его имя дела и привело в ФРГ к серьёзному внутриполитическому кризису, окончившемуся 7 мая 1974 года отставкой Вилли Брандта с поста федерального канцлера.

В 1982 году разведкой ГДР был завербован сержант ВВС США Джеффри Карни, занимавший должность специалиста по коммуникационным проблемам и переводчика в западно-берлинском аэропорту «Темпельхоф». В апреле 1984 года Карни был переведён на базу ВВС в Техасе. В течение двух с половиной лет он переправлял сначала из Темпельхофа, а потом из Техаса копии секретных документов.

Сбежав в 1985 году в ГДР, Карни и здесь продолжал шпионить за своими соотечественниками и их союзниками

в Европе. Он занимался перехватом и дешифровкой засекреченных переговоров между высокопоставленными представителями военных и шпионских ведомств в Западном Берлине. В 1991 году году Карни всё ж таки был арестован и приговорён к 38 годам тюрьмы.

В 1983 году сам предложил свои услуги разведке ГДР уорент-офицер Джеймс Холл, проходивший службу в западном Берлине и имевший доступ к сверхсекретной информации по базе радиоразведки в Тойфельсберге. За 4 года службы в Тойфельсберге Холл передал КГБ сотни сверхсекретных документов, в частности информацию по проекту «Троян» – мировой сети электронного наблюдения.

Затем он служил на американской военной базе в Джорджии. В результате его деятельности была выведена из строя компьютерная программа, нацеленная на определение слабых мест в системе советских военных коммуникаций. В 1989 году Холл был осуждён к 40 годам заключения в военной тюрьме.

В апреле 1981 года подразделение электронной разведки Армии США в ФРГ, известное под названием «Группа быстрого реагирования», осуществило операцию по закладке прослушивающих устройств в автомашины советского военного атташе в ФРГ. При этом в шасси заказанных на заводе фирмы «Опель» в Рюссельсхайме 12 автомобилей установили аппаратуру, которую можно было обнаружить только при разрушении машины. В результате американцы раскрыли несколько советских агентов и дешифровали ряд кодов советской военной разведки.

После появления глобальной сети Интернет в 1980-х годах МО Германии стало уделять должное внимание и компьютерной разведке. Стало известно, что в 2006 году в МО было создано специальное подразделение компьютерных сетевых операций «CNO» (англ. Computer Network Operations), которое базируется в Бонне.

Сотрудники «CNO» прошли подготовку в том числе путём «симуляции кибератак в лабораторных условиях» и сейчас «достигнута способность действовать во враждебных сетях» под военным командованием.

Как сообщает журнал «Spiegel», «BND» стала расширять наблюдение за интернет-пространством и готова потратить на эти цели до 100 миллионов евро. В частности, немецкую службу внешней разведки интересуют соединения с Россией и Восточной Европой.

О секретной программе по расширению интернет-наблюдения глава «BND» Герхард Шиндлер сообщил на встрече с комитетом доверенных лиц бундестага, перед которым

разведслужба отчитывается по бюджету. Программа предусматривает увеличение штата подразделения технической разведки на 100 человек, а также его серьезное переоснащение. Первые 5 миллионов евро на эти цели были выделены «BND» в 2014 году.

Немецкий закон об ограничении тайны переписки, а также почтовой, телеграфной и иной электросвязи (закон «G10») разрешал «BND» проверять до 20% таких сообщений и соединений между Германией и другими странами. Современные компьютерные и серверные мощности позволяют спецслужбе обрабатывать только 5% телефонных звонков, сообщений по электронной почте, обсуждений в «Facebook» и бесед через «Skype».

В 2011 году «BND» проверила почти 2,9 миллиона сообщений «SMS» и электронных писем, переданных за границу или поступивших в ФРГ из-за рубежа. Среди стран и регионов, сообщение с которыми особенно интересует немецкую разведслужбу, Россия, Восточная Европа, африканские конфликтные регионы, Ближний Восток, а также Пакистан и Афганистан.

Сегодня «BND» насчитывает 7 тысяч сотрудников, 2 тысячи из которых заняты непосредственно добычей разведданных. Трудятся они кто в штаб-квартире в Пуллахе, а кто и в 300-х офисах по всему миру. Бюджет организации в 2009 году составлял 460 миллионов евро, а к 2020 году планируется выделение ещё 300 миллионов. Обратим внимание на порядок сумм: то, что предполагается потратить на новую информационную систему, обойдётся в деньги, сопоставимые с годичным бюджетом госструктуры в целом. Такова роль современных информационных технологий в развитых государствах.

Новый киберпроект назван «Анализом потоковых данных в режиме реального времени» и осуществляется в рамках «Стратегической технологической инициативы». Уже в 2014 году она позволила «BND» взять под пристальное наблюдение блоги, форумы и порталы, такие как «Flickr», «Facebook» и «Twitter». Считается, что именно их пристальный мониторинг даёт наиболее полное и точное представление о ситуации за рубежом.

Методические основы такой работы были разработаны в ходе проводимого Мюнхенским университетом Бундесвера исследовательского проекта «Автоматизированное обозрение интернет-контента». Планировалось установить современное оборудование сбора метаданных и новейшие системы биоидентификации. И то, что действия «BND» находятся под

пристальным вниманием защищающего личную жизнь и приватность Верховного суда в Карлсруэ, ничуть такому техническому перевооружению не мешает.

Также, благодаря утечке официальных документов через сайт «WikiLeaks» стало известно, что правоохранительные органы Германии закупают и устанавливают в компьютеры подозреваемых специальную шпионскую программу для прослушивания телефонных разговоров через «Skype» и перехвата шифрованных «SSL» – соединений.

Разработчиком программы под названием «Модуль захвата Скайпа» (англ. Skype Capture Unit) была баварская компания «DigiTask» из города Хайген. Цена изделия и его обслуживания была очень высокой: всего 3 месяца (минимальный срок) работы шпиона на одном компьютере обходились правоохранительным органам в 20,5 тысяч евро.

«Digitask» предложила скрытую установку ПО, его массовую рассылку по «e-mail» или целевую установку прямо на необходимый компьютер. Установленный модуль становится своеобразным посредником. Все входящие и исходящие разговоры сначала проходят через удаленный сервер, записывающий информацию.

А в целом, согласно другому документу, лишь одно германское Бюро таможенных расследований, к примеру, закупило у компании «DigiTask» шпионских услуг на сумму более 2-х миллионов евро.

В апреле 2016 года Германия приступила к процессу создания Командования в компьютерном и информационном пространстве «KCIR» (нем. Kommando Cyber und Informationsraum). Оно объединяет все существовавшие ранее подразделения, работавшие в этой области, а также несет ответственность за информационную и кибербезопасность, военную разведку, системы геоинформирования и позиционирования, а также оперативные коммуникации.

1 апреля 2017 года эта структура была введена в действие и ее возглавил офицер в звании генерал-лейтенанта. В состав «KCIR» вошли 13,5 тысяч служащих, которые на момент создания уже служили в других военных и армейских подразделениях. Они были расквартированы в двух новых центрах:

– Центр кибероперации (англ. Cyber operations centre),

– Центр кибербезопасности Бундесвера (англ. Bundeswehr cyber security centre).

МО Германии также объявило, что оно стремится к тому, чтобы у Бундесвера были ресурсы и возможности для нанесения ответного удара в случае необходимости, что позволит «KCIR»

работать на том же уровне, что и другие страны, например, США. Департамент информации и компьютерных сетевых операций (англ. Department of Information and Computer Network Operations) в рамках Стратегического разведывательного подразделения Бундесвера (англ. Bundeswehr's Strategic Reconnaissance Unit), в основном, концентрируется на расширении оборонных возможностей.

После серьезного анализа законодательства, проведенного в начале 2000-х годов, МО в 2005 году приступило к попыткам разработки наступательных технологий, например, собственных «красных» команд хакеров (англ. red teams), отдавая себе отчет в том, что опыт использования такого секретного кибероружия может быть использован исключительно в целях обороны.

Правительство Германии стремится к тому, чтобы оборонные мероприятия не смешивались с разведывательной деятельностью. В 2011 году правительство создало Национальный центр киберреагирования в составе Министерства внутренних дел. Этот центр объединяет ресурсы различных правительственных организаций, в том числе – федеральной уголовной полиции и службы внешней разведки, а также ресурсы частного бизнеса.

21 октября 2016 года федеральное собрание «Бундестаг» приняло закон, который предусматривает значительное расширение полномочий разведки «BND». Теперь она сможет контролировать не только иностранцев, но и жителей своей страны. Служба была лишена такого права в середине прошлого века, когда была одержана победа над нацистами.

Предусмотрено и увеличение масштаба прослушки. Раньше «BND» имела право собирать лишь 20% трафика одного из крупных интернет-каналов, теперь же она сможет прослушивать 100% трафика всех интернет-каналов.

Прежде спецслужбы могли контролировать граждан только в 8 целях, среди которых борьба с терроризмом, киберпреступность и незаконная торговля людьми. Закон расширил цели, например, контролировать граждан Германии с целью сбора сведений внешнеполитического значения.

Поводом для проверки коммуникаций теперь могут стать не чёткие формулировки о подозрениях в терроризме и т. д., а размытые определения о сведениях, «имеющих значение с точки зрения политики безопасности».

Помимо сбора персональных данных, полномочия «BND» расширены и в вопросах сбора метаданных коммуникаций. Например, кто с кем говорил, когда и как долго, с какого именно телефона и где в этот момент находился. Теперь для этого не понадобится иметь какие-либо основания – в категорию

потенциально прослушиваемых попадут все, кого «нельзя однозначно идентифицировать как граждан Германии».

Критики считают, что такая формулировка оставляет возможности для сбора информации практически о любом человеке. Напомним, согласно исследованиям учёных Стэнфордского университета, метаданные коммуникаций человека способны рассказать о нем настолько много, что проводить мероприятия наблюдения за ним в некоторых случаях и не нужно.

Плюс к этому, при «двухпрыжковом» методе сбора метаданных, за ним потянутся метаданные ещё около 25 тысяч абонентов, которые могу быть вообще никак с ним не связаны, но, тем не менее, их личная тайна может стать доступна спецслужбам. «Один прыжок» означает, что подозреваемый А вызывает человека Б, а «второй прыжок» – человек Б вызывает человека В.

10. Радиоразведка Франции

К моменту изобретения радио Франция была в числе крупнейших военных держав мира и лидеров военно-технического развития, поэтому уже в начале XX века радиосвязь была поставлена на службу французской армии. Накануне Первой Мировой войны во Франции были сформированы первые подразделения, перед которыми были поставлены задачи радиоразведки и радиоперехвата.

Накануне Первой Мировой войны французам удалось вскрыть военные и дипломатические шифры Германии и Италии. Французская военная криптослужба «Комиссия по военным шифрам» под руководством Франсуа Картье имела возможность читать зашифрованные радиограммы, которыми немцы обменивались во время маневров. Кроме того, агентура, дезертиры из германской армии и лица, завербованные в Иностранный легион, постоянно снабжали комиссию информацией.

В начале войны французские станции радиоперехвата находились лишь в 3-х специальных пунктах и в больших крепостях. К тому же немцы на своей территории пользовались телеграфными линиями. Поэтому материала для дешифровки было немного. Но когда немцы вторглись на французскую территорию, им пришлось перейти на радиосвязь, и возможности радиоперехвата возросли.

А когда к пунктам радиоперехвата добавилась Эйфелева башня, они стали почти безграничными. Немецкие радиограммы ложились на стол Картье почти одновременно с тем, как они докладывались немецким генералам. Более 100 миллионов слов перехватили за годы войны сотрудники Комиссии.

По характеру и частоте переговоров, даже без их дешифровки, радиоразведка научилась различать рода и боевые порядки войск, уровни штабов, подготовку противника к наступательным действиям и т. д. Но, естественно, значительно больше информации давала дешифровка радиопередач.

Был, например, раскрыт шифр немецких ПЛ. Вскоре радиопеленгаторы засекли передачи шпионской немецкой радиостанции, разместившейся в городе Науне на берегу Средиземного моря. Она сообщала немецким ПЛ маршруты и время выхода французских судов из Марселя. Не составляло особого труда контрразведке найти и обезвредить эту радиостанцию.

Но французы поступили иначе. После перехвата шпионских

шифртелеграмм их направляли для дешифровки, на что требовалось не более часа. Затем их содержание сообщалось начальнику марсельского порта. У него оставалось время, чтобы изменить расписание рейсов и ввести немцев в заблуждение. Судам, которые уже вышли в море, давали распоряжение об изменении курса.

Боевым дебютом и одновременно самым большим и важным успехом в истории французской службы радиоперехвата стала ее работа в сентябре 1914 года, во время битвы на Марне. Своевременно перехваченные и дешифрованные Комиссией радиосообщения немецкой армии позволили ГШ генерала Жозефа Жоффра выявить намерения и направление ее удара, а также дали информацию о трудностях, с которыми она столкнулась в ходе своего наступления.

Полученные радиоразведкой сведения позволили французам нанести контрудар и вынудить немцев начать отход. Так был спасен Париж и сорван план немецкого генерал-фельдмаршала Альфреда фон Шлиффена, предусматривавший быстрый разгром Франции в ходе молниеносного наступления за счет упреждающей мобилизации. В результате война стала затяжной позиционной, в которой получившие передышку союзники смогли переломить ход событий и в конце концов одержать победу.

Своими достижениями в сфере криптоанализа французы делились с главным союзником – Великобританией, отправляя туда многие из раскрытых шифов Германии. Однако британцы не всегда отвечали взаимностью. Был случай, когда, имея возможность предупредить французов об угрозе торпедирования их катера, британцы не сделали этого.

При этом руководитель военно-морской разведки Уильям Генри Холл заявил: «Лучше потерять корабль, чем рисковать тем, что о существовании нашей криптоаналитической службы стало бы известно немцам».

Угроза провала всегда существовала для сотрудников криптослужбы. Например, благодаря дешифровке немецких переговоров французы узнали о предстоящем визите в город Тилт (Бельгия) кайзера Вильгельма и организовали бомбежку города как раз в момент его прибытия.

Об этом событии известила французская газета «Le Matin», не забыв упомянуть и об источнике информации. Конечно, это была непростительная оплошность французских служб безопасности и контрразведки. Поскольку прочитав газету, немцы сразу же перешли на новую шифрсистему. Только из-за небрежности немецких шифровальщиков французским криптоаналитикам удалось ее раскрыть всего через месяц.

Вообще, немецкие связисты далеко не всегда были скрупулезны в исполнении своих обязанностей. В первые месяцы войны, опьяненные легкими победами и утомленные однообразной криптологической работой, они начали передавать многие сообщения частично открытым текстом. Иногда французы специально провоцировали их, якобы готовясь перейти в контрнаступление, чтобы немцы включали в открытые тексты необходимые французским криптоаналитикам слова.

Часто связисты ленились менять стереотипные фразы вроде «ночь прошла спокойно», «потерь нет» и т. п. В качестве проверочных сообщений немцы, вводя в действие новую шифрсистему, нередко использовали одну и ту же пословицу: «Ранней пташке достается червяк», аналогичную нашей: «Кто рано встает, тому Бог дает». Все эти недостатки упрощали работу французских криптоаналитиков.

Комиссия также оказывала помощь МИД в вопросах чтения дипломатической шифрованной переписки на линии Берлин – Мадрид. Именно в результате радиоперехватов французские спецслужбы узнали о немецком агенте «Н-21», которой была Мата Хари. Как известно, она была арестована, осуждена и расстреляна 15 октября 1917 года.

Самым большим успехом французской службы радиоперехвата и дешифровки стало предупреждение командования о «последнем решительном» наступлении немцев на западном фронте, которое они развернули 7 июня 1918 года. Французы сумели вовремя перестроить резервы, и немецкое наступление захлебнулось. До конца войны оставалось 5 месяцев, и немцы так и не смогли оправиться от своего провала.

Победная эйфория, охватившая французское общество и вооруженные силы, оказала большое негативное влияние на развитие службы радиоразведки в межвоенный период. Уверенность в непоколебимости «Линии Мажино» как главном инструменте обеспечения национальной безопасности привела к тому, что одна из самых мощных и хорошо оснащенных в 1918 году служб радиоразведки ощутимо деградировала к 1940 году и практически не сыграла сколько-нибудь важной роли во Второй Мировой войне.

Однако по мере приближения новой войны с Германией Разведуправление Генштаба ВС Франции значительно активизировало свою работу, снабжая Генштаб данными о тактике немецкого «блицкрига».

Практически самостоятельно действующее с 1936 года одно из его подразделений – Информационная служба (фр. Service de Renseignement), имевшая в своем подчинении разветвленную сеть

станций прослушивания, активно перехватывала радиосообщения, передававшиеся из Германии, Италии, Испании и других европейских государств.

В 1941 году бригадный генерал Шарль де Голль создал в Лондоне новую службу разведки Франции, вскоре получившую название «Центральное бюро информации и действия» (фр. Bureau Central de Ren-seignements et d'Action).

В ноябре 1942 года после высадки англоамериканских войск в Северной Африке, по указанию де Голля на базе центрального бюро и службы информации была создана новая спецслужба – Главное управление специальных служб (фр. Direction General des Services Specieux). Служба информации вошла в нее на правах технического отдела.

В 1944 году оно было переименовано в Главное управление изучения и исследований (фр. Direction General des Etudes et Recherches), однако просуществовало до января 1946 года. Причиной тому были многочисленные злоупотребления сотрудников этой службы, в том числе связанные с незаконным прослушиванием телефонов и перлюстрацией корреспонденции сотен тысяч французов, подозреваемых в антигосударственной деятельности.

Как только де Голль ушел с должности президента Франции, главное управление мгновенно расформировали, а вместо него создали Службу внешней документации и контрразведки «SDECE» (фр. Service de Documentation Exterieure et de Contrespionage).

Следующей важной вехой в развитии французской службы радиоразведки стоит считать войну в Индокитае (1946—54). После Второй мировой войны между Францией и вьетнамским движением за независимость Хошимина, которому во время оккупации полуострова с 1940-го по 1945-й год покровительствовали японцы, а позже Чан Кайши, разгорелся конфликт. Радиоперехват источников противника снабжал командование французского экспедиционного корпуса и верховный комиссариат важной информацией.

В 1948 году в Сайгон и Ханой прибыла отдельная рота радиоперехвата и радиопеленгации «CAER», развернув там узел радиоперехвата и сеть из 8 полустационарных пеленгаторов, распределенных по полуострову, которую усилили 2-мя подразделениями мобильных пеленгаторов. Рота стала частью развернутой группировки радиоэлектронного контроля на Дальнем Востоке «DR GCR EO».

Поддержку в области криптоанализа и дешифровки подразделению оказывала техническая служба разведки «STR». «STR» и «GCR», в свою очередь, являлись подразделениями

«SDECE» созданной в первые послевоенные годы новой французской разведывательной спецслужбы. Основной задачей роты «CAER» в том конфликте были радиоразведка и радиоперехват.

После завершения войны в Индокитае большая часть личного состава «CAER» присоединилась к французским силам в Германии и влилась в 42-й полк связи, став солдатами и офицерами 708-й роты радиоперехвата и радиопеленга.

Следующим боевым эпизодом после Индокитая для французской радиоразведки стал Алжир. В период 1956—62 годов 708-я рота, которая после реорганизации стала именоваться 708-й ротой связи, перехватывала радиосообщения Фронта национального освобождения в Алжире, Тунисе и Марокко.

По прибытии из Алжира личный состав подразделения вернулся в 42-й полк и принял участие в «холодной» войне. Теперь основным вероятным противником стали гораздо лучше оснащенные, чем алжирские повстанцы, вооруженные силы стран Организации Варшавского договора (далее – ОВД) и прежде всего СССР. В связи с этим 1 ноября 1967 года после серии различных реорганизаций был создан 708-й батальон.

Его основной задачей было ведение радиоразведки многочисленных источников электромагнитного излучения на территории ГДР и Чехословакии. Средства и личный состав батальона были развернуты в основном в ФРГ, объектами их работы стали РЭС подразделений Группы советских войск в Германии, а также войск ГДР и Чехословакии.

Объем работы батальона постоянно рос по мере насыщения войск потенциальных противников средствами связи и развития сети РЛС в странах Варшавского договора. Поэтому 1 октября 1971 года 708-й батальон РЭБ был переформирован в 44-й полк связи. Стоит отметить, что спецификой французского понимания РЭБ на протяжении большей части холодной войны оставалось ведение радиоразведки и радиоперехвата.

Это касалось как сухопутных войск, так и авиации и флота. Например, в состав ВМС Франции с мая 1977 года входило разведывательное судно «Berry», оснащенное аппаратурой радиоэлектронной разведки и предназначенное для ведения радиотехнической разведки РЛС и средств связи кораблей и судов ВМФ СССР преимущественно в Средиземном море.

Радиоэлектронное подавление как важнейшая составляющая РЭБ стало частью французской концепции «электронной войны» только в 1980-х годах под влиянием анализа опыта ближневосточных (прежде всего арабо-израильских) конфликтов.

Результатом стало появление в ВС Франции нового 54-го полка связи. В задачи полка вошли радиотехническая разведка и радиоэлектронное подавление.

2 апреля 1982 года Служба внешнего осведомления и контрразведки «SDECE» (фр. The Service de Documentation Extérieure et de Contre-Espionnage) МО Франции была реорганизована в Главное управление внешней безопасности «DGSE» (фр. Direction générale de la Sécurité extérieure). В его задачи входят следующие мероприятия:

1. Зарубежная агентурная и оперативно-техническая разведка:

– техническая разведка включает в себя перехват и перлюстрацию секретных документов иностранных государств, слежение за системами связи и дешифровка перехваченных сообщений;

2. Радиоэлектронная разведка (далее – РЭР) за рубежом:

– система РЭР «Frenchelon»;

– перехват и дешифровка электронных сообщений по запросу спецслужб, полиции и жандармерии, по которым ГУВБ МО взаимодействует с управлением государственных шифров «PNCD» (фр. Pôle national de cryptanalyse et décryptement) МО;

– спутниковая видовая разведкя и РЭР;

– электронная разведка и перехват данных в общественных компьютерных сетях;

3. Анализ политической и военной информации из открытых источников;

4. Обмен информацией с другими спецслужбами Франции, дружественных государств и государств НАТО;

5. Спецоперации за рубежом.

В структуру «DGSE» входят следующие Управления:

– Оперативно-плановое «DS» (фр. La direction de la stratégie);

– Главное управление разведки «DR» (фр. La direction du renseignement);

– Спецопераций «DO» (фр. La direction des opérations);

– Оперативно-техническое «DT» (фр. La direction technique).

ОТУ «DT» на 2000 год имело в своем состав 3 отдела:

– технических разработок: РЭР, взлом компьютерных систем, шифрование и дешифрование;

– информационных технологий и связи;

– оперативной техники: техническая поддержка, специальная техника, обработка изображений.

Сегодня «DGSE» располагает сетью станций РЭР в Куру (Французская Гвиана), некоторые из них эксплуатирует совместно с Управлением военной разведки Франции и Службой внешней

разведки ФРГ.

Управление военной разведки «DRM» (фр. Direction du renseignement militaire) было создано в июне 1992 года на основе полученного боевого опыта в Персидском заливе. Теперь эта подведомственная МО служба стала ответственна за сбор информации, анализ и координацию разведывательной деятельности всех видов вооруженных сил (далее – ВС) Франции.

«DRM» возглавляет директор, который является офицером одного из видов вооруженных сил и подчиняется начальнику ГШ ВС Франции. Штаб-квартира УВР находится в Париже, а подразделения технической разведки – в Крейле (40 километров к северу от Парижа) и Страсбурге.

Что касается получения разведданных с помощью технических средств, то «DGSE» отводилась главная роль делать это путем радиоперехвата, а «DRM» – путем добывания и обработки сведений от спутниковых средств оптоэлектронной разведки.

Ответственность за добывание стратегических разведданных с помощью радиоэлектронных средств и ее анализ несет Техническое управление «DGSE». Его работа заключается в организации и осуществлении дешифровки, прослушки телефонных переговоров, сборе и анализе разведданных от широкой сети станций радиоперехвата (около 100 технических пунктов), размещенных на своей территории и в различных регионах мира.

В Крейле также базируются Центры подготовки специалистов РЭР и коллективного пользования данными разведывательного спутника «Helios». Эта спутниковая система является совместным проектом Франции, Италии и Испании, а ее управление осуществляется в соответствии с вкладом каждой из стран: 79% – Франция, 14% – Италия и 7% – Испания.

«DRM» после соответствующей реорганизации получило в подчинение все разведывательные подразделения. Так, 1 сентября 1993 года в составе Сухопутных сил была создана бригада радиоразведки, в состав которой вошли 44-й (радиоразведка) и 54-й (радиотехническая разведка) полки связи.

«DRM» был подчинен новый корабль радиоразведки «Dupuy-de-Lome», вступивший в строй в 2006 году, спроектированный и построенный специально для ведения РЭР в интересах «DRM». Радиоэлектронное оборудование «Dupuy-de-Lome» включает в себя две навигационные РЛС «DRBN-38A», станции спутниковых систем связи «Syracuse» and «Inmarsat», станцию предупреждения о радиолокационном облучении и идентификации РЛС «ARBR-21», комплексы радиоразведки.

Последние позволяют обнаруживать, пеленговать и проводить технический анализ излучений различных РЛС в диапазоне частот от 300 МГц до 90 ГГц, а кроме того, перехватывать, пеленговать и прослушивать сигналы систем связи (включая спутниковые) в диапазоне частот от 30 кГц до 100 ГГц.

Французские специалисты утверждают, что оборудование корабля позволяет перехватывать и анализировать любые типы сигналов, включая сообщения электронной почты и разговоры по мобильным телефонам

Корабль является частым гостям в акваториях различных конфликтов. Так, в апреле 2014 года «Dupuy-de-Lome» присутствовал в акватории Черного моря недалеко от берегов Крыма, ведя радиоразведку российских сил, переброшенных на полуостров.

ВВС Франции в своем составе имеет 54-ю эскадрилью, базирующуюся в Дюнкерке и имеющую на вооружении два самолета радиоразведки C-160G «Gabriel».

Наземную, воздушную, морскую компоненту «DRM» дополняет космическая. Франция периодически обновляет группировку спутников радиоразведки. К 2020 году планируется запуск спутниковой системы «CERES» (фр. Capacite de Renseignement Electromagnetique d'origine Spatiale – возможность разведки электромагнитного пространства), которая будет состоять из 3-х или 4-х микроспутников радиоразведки.

В настоящее время важнейшим направлением развития войск радиоразведки Франции считается совершенствование их возможностей по пеленгации и перехвату средств связи, используемых террористическими исламистскими группировками.

Совсем недавно в Мали в ходе операций «Сервал» и «Бархан» два местных руководителя «Аль-Каиды»[1] и движения «Ансарр Эддин» были ликвидированы французским спецназом благодаря работе такого вида радиоразведки, как идентификации и пеленгации сотовых и спутниковых телефонов.

Для Франции, основная угроза национальной безопасности которой исходит от исламистов и которая не имеет выраженных военных угроз от высокотехнологичных держав, развитие средств радиоперехвата и радиоразведки, а также средств постановки помех радиоуправляемым взрывным устройствам имеет приоритетный характер.

Франция располагает собственной глобальной системой РЭР «Frenchelon» (аналог американской системы «Эшелон» и русской системы «СОУД»), которая находится в ведении «DGSE» и УВР. Крупнейшая станция этой системы расположена в Домме

(департамент Дордонь, регион Аквитания), а помимо этого, имеется разветвлённая инфраструктура РЭР как на территории Франции, так и за рубежом и в бывших колониях.

Так, например, зарубежные станции расположены в следующих населенных пунктах: Сен-Бартелеми, Джибути, Реюньон, Куру, Папеэте, Тонтута (Новая Каледония) и Майотта (станция была закрыта в 1998 году).

Эти станции способны перехватывать электронные сообщения и дешифровывать закодированные сообщения дипломатического, военного или промышленного происхождения. Интересно, что несмотря на многочисленные публикации в СМИ, официальные власти Франции никогда не подтверждали существование системы «Frenchelon».

Кроме того, ВС Франции используют также систему РЭР «Emeraude» (фр. Ensemble mobile écoute et recherche automatique des émissions – мобильный набор автоматического поиска и прослушки излучений), которую часто путают с системой «Frenchelon».

Инфраструктура системы «Emeraude» позволяет решать широкий круг задач, выходящих за рамки прослушки. В частности, может быть использована в интересах сил гражданской обороны и гражданских или военных властей, ответственных за внутреннюю безопасность. Она может быть использована для перенаправления телефонных звонков в экстренные службы в условиях чрезвычайных ситуаций, стихийных бедствий или перегрузки «call» – центров.

«Emeraude» связана со всеми государственными и частными телекоммуникационными компаниями, провайдерами и операторами связи (включая проводное, беспроводное и радиовещание), ведущими свою деятельность на территории Франции, и может перехватить переговоры любого абонента их сетей.

Станции радиоперехвата, входящие в «Emeraude» и развернутые вблизи Центра управления и эксплуатации РЭБ, выполняют следующие задачи:

1) в радиоразведке:

– радиоперехват и прослушивание передач в УКВ диапазоне, в частности, с использованием радиоперехватчика системы «SAIGON ARBG 1»;

– перехват аналоговой радиорелейной связи;

– перехват и автоматический анализ характера радиосообщений (передача данных, взрыв и т. д.).

2) в радиотехнической разведке:

– перехват излучения радаров противника, в частности,

с помощью перехватчика радара «ARBR21».

«DGSE» систематически перехватывает электромагнитные сигналы, передаваемые по телефонным и компьютерным сетям внутри Франции и из Франции за границу. Полученные подобным образом метаданные электронной почты, «SMS», телефонных звонков, активности на «Facebook» и «Twitter» впоследствии хранятся в течение многих лет.

Огромной базой данных без каких бы то ни было законных оснований и контроля тайно пользуются все разведывательные службы Франции. Данная программа фигурирует в ряде парламентских документов. Так, в докладе парламентского Комитета по делам разведки от 30 апреля 2013 года говорится, что «с 2008 года были достигнуты успехи в распределении возможностей, в частности, касающихся электроразведки, осуществляемой „DGSE“ в пользу всего разведывательного сообщества».

Миллиарды перехваченных данных затем сжимаются и хранятся на 3-х подземных этажах в штаб-квартире «DGSE» на бульваре Мортье в Париже. Полученные метаданные позволяют строить огромные графики связей между людьми, своеобразные дневники телефонной и компьютерной активности каждого гражданина.

Технический директор Управления Бернар Барбье дважды публично упоминал о данной практике. В ходе одного из этих выступлений он говорил о «создании ЭВМ на базе программируемой пользователем вентильной матрицы», способной обрабатывать десятки петабайт информации.

Помимо самого «DGSE» к базе данных имеют доступ 6 разведывательных служб Франции: УВР, Управление защиты и безопасности обороны, Центральное управление внутренней безопасности, Национальный директорат разведки и таможенных расследований, Управление разведки и противодействия подпольным финансовым схемам «Tracfin», а также разведслужба полицейской префектуры Парижа.

Кроме того, в 2010 году между «DGSE» и британским ШКПС было подписано тайное соглашение о сотрудничестве в сфере перехвата информации.

11. Содружество радиоразведок

22 февраля 1946 года в Лондоне прошла конференция стран Содружества по вопросам сотрудничества в области радиоразведки. В ней приняли участие Великобритания, Канада, Австралия и Новая Зеландия. На конференции Австралия предложила в качестве своего вклада в создание радиоразведывательного союза 4-х стран-участниц конференции предоставлять им материал с 65 австралийских станций радиоперехвата.

Конференция стала прелюдией к переговорам с американцами месяц спустя, на которых австралийцы и канадцы уполномочили британцев выступать от их имени. 6 марта 1946 года из США в Лондон прибыл американский криптолог Уильям Фридман, который с 1943 года был ответственным за сотрудничество между американской и британской службами разведки в сфере коммуникаций.

Еще 17 мая 1943 года британской и американской службами радиоразведки и дешифровки было подписано соглашение «BRUSA agreement» (англ. BR – Британия, USA – США), которые составил Фридман. Это было соглашение спецслужб Великобритании и США по обмену разведывательной информацией, которое оговаривало обмен сотрудниками и совместные правила для обработки и распределения критически важных данных во время войны.

После окончания Второй Мировой войны надо было согласовать новое 4-страничное соглашение взамен прежних соглашений об англо-американском сотрудничестве в области радиоразведки. К этому соглашению прилагались несколько дополнений, разработанных в ходе подготовительной рабочей встречи английских и американских дешифровщиков.

Дополнения в основном касались процедур защиты добываемой радиоразведкой информации. В соглашении договаривающиеся стороны брали на себя обязательства обмениваться данными о зарубежных службах радиоразведки и хранить в строжайшей тайне сведения о сотрудничестве друг с другом в сфере радиоразведки.

В результате в 1946 году было подписано новое соглашение Великобритании и США о сотрудничестве в области РЭР, названное как «UKUSA agreement» (англ. UK – United Kingdom – Соединённое Королевство Великой Британии).

Участники Содружества согласились на обмен данными относительно следующих мероприятий, связанных

с иностранными коммуникациями: сбор трафика; приобретение средств связи, документов и оборудования; анализ трафика; криптоанализ; дешифровка и перевод; получение информации относительно сообщений, организации, процедур, методов и оборудования.

В январе 1947 года состоялась следующая конференция стран Содружества, посвященная сотрудничеству в области РЭР. На ней Великобритания заявила о своем согласии на присоединение Австралии к англо-американскому радиоразведывательному союзу – соглашению «UKUSA agreement».

В ходе переговоров британцев с американцами было решено, что стратегическим направлением англо-американского сотрудничества в области РЭР станет ускоренная переориентация на перехват и чтение советской радиопереписки. После окончания Второй Мировой войны британские станции радиоперехвата и в Великобритании, и за ее пределами переключились на советский радиоперехват.

Именно это, как надеялись британцы, сделает их привлекательными партнерами для сотрудничества с американцами в области РЭР, главной целью которого в ближайшее время должна была стать атака на советские шифрсистемы. Криптоаналитики Блетчли Парка Джон Тилтман и Хью Александер должны были поделиться с американцами своим богатым опытом в этой области, а американцы, в свою очередь, предоставить оборудование для автоматизации взлома советских шифров.

«UKUSA agreement» периодически продливался и сегодня включает в себя, помимо Великобритании и США, Канаду (1948), Австралию (1956) и Новую Зеландию (1956). В работе Содружества в качестве «третьей стороны» участвуют Норвегия (1952), Дания (1954), ФРГ (1955), а также Япония, Южная Корея, Израиль, ЮАР, Малайзия, Сингапур и страны-участники НАТО.

Одним из наиболее известных проектов, осуществляемых под эгидой «UKUSA», является создание и эксплуатация глобального комплекса радиоэлектронной разведки «Эшелон» (англ. Echelon).

В деятельности Содружества активно участвуют следующие спецслужбы:

– США – Агентство национальной безопасности, АНБ (англ. National Security Agency, NSA),

– Великобритания – Штаб-квартира правительственной связи, ШКПС (англ. Government Communications Headquarters, GCHQ),

– Австралия – Управление радиотехнической обороны (англ. Defence Signals Directorate, DSD),

– Новая Зеландия – Бюро безопасности правительственных

коммуникаций (англ. The Government Communications Security Bureau, GCSB),

– Канада – Ведомство безопасности коммуникаций (англ. Communications Security Establishment, CSE).

Каждый из участников «UKUSA» несёт ответственность за сбор и анализ информации в различных регионах мира:

– США – страны Латинской Америки, азиатская часть России и север Китая,

– Канада – Южная и Центральная Америка и северное побережье России,

– Великобритания – страны Европы (включая европейскую часть России) и страны Африки,

– Австралия – регион Индокитая, Индонезия, южные и центральные регионы Китая,

– Новая Зеландия – Западная и Южная части Тихоокеанского региона.

Совместная работа всех органов радиоразведки координируется Организацией комплексного перехвата сигналов (англ. *Complex Signal Organization, CSO)*. Большинство станций, работающие в интересах «*CSO*» и военных баз и находящиеся на территории Великобритании, входят в состав МО, и только станция в Морвенстоуне подчинена ШКПС. Для специальных контактов АНБ с Великобританией в рамках Соглашения UKUSA Агентство располагает в Лондоне Бюро по специальным связям «Special United States Liaison Office» (SUSLO).

Британцы регулярно отсылали в Вашингтон, а таже всем 3-м видам вооруженных сил радиоразведывательные информационные сводки, составленные на основе перехваченной и прочитанной советской переписки. Уже 28 апреля 1948 года генерал Чарльз Кабелл, начальник военно-морской разведки США, с удовлетворением отметил: «В настоящее время налажен полномасштабный обмен радиоразведывательной информацией в отношении Советской России между заинтересованными спецслужбами Англии и США».

Взаимоотношения США с другими странами Содружества в области радиоразведки тоже не отличались особой теплотой. Сотрудничество с Канадой развивалось очень медленными темпами. Более того, американцы подозревали, что британцы тайно делятся с канадцами радиоразведывательной информацией, которую получали от США.

Американские дешифровщики очень не хотели, чтобы добываемая ими информация безо всяких ограничений распространялась среди всех заинтересованных в ее получении

лиц. Особую озабоченность у американцев вызывал отказ канадцев принять у себя стандартные меры безопасности, которые действовали в США для сохранения радиоразведывательной информации в строжайшей тайне.

В результате переговоры США с Канадой по поводу сотрудничества в области радиоразведки тянулись без особого успеха аж до 1953 года. Не лучше обстояли дела во взаимоотношениях США с Австралией, где в конце 1940-х годов разразился ряд скандалов, связанных с разоблачением агентов советской разведки в ходе проведения криптоаналитической операции «Венона».

В 1960-е годы методы ведения радиоразведки претерпевали быстрые и значительные изменения, связанные с новым источником разведывательных данных. Обратить внимание на этот источник заставили проблемы со взломом шифраторов высокой стойкости, а также произошедшая революция в области телекоммуникаций.

В это время на смену телефонным проводам стали приходить радиолинии, использовавшие микроволновые ретрансляторы и спутники. Беспроводная связь оказалась значительно более эффективной для междугородных и международных телефонных звонков.

Службы радиоразведки по достоинству оценил один из побочных эффектов этого перехода на беспроводную связь. Состоял он в том, что радиосигналы распространялись совершенно бесконтрольно, что позволяло их легко перехватывать. Было удобно и то, что большинство телефонных переговоров по радиоканалам осуществлялось в незашифрованном виде.

Правда, были и недостатки. Во-первых, вскоре радиоперехват возрос до таких объемов, что персонал уже не справлялся с его обработкой и анализом. Тогда на помощь аналитикам радиоразведки были призваны компьютеры, которые стали использоваться не только для взлома шифров, но и для отбора полезной радиоразведывательной информации, ее хранения, анализа и предоставления для ознакомления заинтересованным пользователям.

Во-вторых, крупные комплексы радиоразведки с их спутниковыми антеннами, которые применялись для перехвата радиосигналов, легко могли послужить предметом излишнего любопытства со стороны иностранной разведки и «желтой» прессы. Все же, несмотря на это, вплоть до середины 1970-х годов удавалось выдавать свои станции радиоперехвата за обычные ретрансляторы, скрывая от публики их истинное назначение.

Чтобы гарантировать себе возможность полноценно пользоваться плодами революции в сфере телекоммуникаций, АНБ и ШКПС организовали ряд совместных тайных операций, одна из которых была связана с прослушкой телефонных разговоров на территории Великобритании.

Так, в 1967 году в Корнуолле по соседству с приемной станцией спутниковой системы связи «Intelsat» ШКПС построила собственную копию этой станции для перехвата сигналов, транслируемых спутниками связи. За оборудование и инфраструктуру заплатило АНБ, а ШКПС осуществляла эксплуатационные расходы и арендную плату за землю.

Другая операция была направлена против коммунистической Кубы в 1969 году. Дело в том, что в 1960-е годы АНБ добывало значительную часть радиоразведывательной информации из телефонных разговоров между Кубой и кубинскими эмигрантами, проживавшими в американской Флориде.

С помощью своих кораблей радиоразведки американцы также могли следить за звонками из Гаваны, столицы Кубы, в другие районы острова. Эта информация представляла определенный интерес для ФБР, которое охотилось за агентами кубинской разведки, работавшими в США под эмигрантским прикрытием.

Большинство прослушанных кубинских разговоров по телефону велись посредством тропосферной радиолинии, принадлежавшей Кубинской радиокорпорации, которая до 1959 года являлась дочерней компанией американской корпорации «ITT», но была национализирована сразу после прихода Фиделя Кастро к власти. К концу 1960-х годов используемое кубинцами оборудование устарело и износилось. Американцы опасались, что оно скоро выйдет из строя, и АНБ лишится ценного источника радиоразведывательной информации.

США могли предложить кубинцам новое оборудование, но были обязаны осуществлять экономическую блокаду Кубы. Чтобы не вызывать у кубинцев никаких подозрений, США обратились за помощью к Великобритании, у которой эмбарго на торговлю с Кубой отсутствовало. В ШКПС обрадовались представившейся возможности оказать услугу АНБ в надежде сделать своих американских коллег более сговорчивыми при решении других вопросов.

Необходимое оборудование было доставлено в Великобританию и оттуда было перенаправлено на Кубу. АНБ гарантировало, что американские поставщики оборудования не будут преследоваться по закону за нарушение эмбарго. А «ITT» использовало свою английскую дочернюю компанию в качестве

ширмы для продажи оборудования кубинцам.

Благодаря откровениям бывшего техника канадского Центра безопасности коммуникаций (далее – ЦБК) Майка Фроста, стало известно, что в 1960 году, когда Президент Франции Шарль де Голль создал общее движение за независимость с франкоязычным Квебеком, ЦБК привлек норвежские, датские, и шведские органы радиоразведки для того, чтобы вести перехват коммуникаций между Парижем и партией Премьер-министра Квебека Рене Левеска с его сепаратистским движением. Кроме того, ЦБК прослушивал телефон в машине посла США в Оттаве, причем курирующие офицеры АНБ были в полной мере осведомлены об этом.

В 1970-е годы только СССР и США обладали технической и финансовой возможностью вести радиоразведку из космоса с помощью спутников. К этому «спутниковому» клубу очень хотела присоединиться Великобритания, и ей удалось это сделать, правда, в довольно специфической области – в использовании спутников для передачи радиоразведывательной информации к месту ее дальнейшей обработки и для связи с АНБ.

Дело в том, что в начале 1950-х годов связь между АНБ и ШКПС была очень плохой, в основном, из-за недостаточной пропускной способности коммуникационных каналов и отсутствия свободных радиочастот. В середине 1950-х годов дело доходило до того, что спецслужбы не могли связаться друг с другом по несколько часов в сутки.

В начале 1970-х годов от этих многочасовых сбоев в межведомственной связи ШКПС и АНБ удалось хотя бы частично избавиться путем ввода в эксплуатацию правительственной спутниковой системы связи «SkyNet». Главным пользователем этой системы стала ШКПС.

Однако ей все равно не хватало пропускной способности спутниковых каналов связи для обмена радиоразведывательной информацией с Австралией, Канадой и США. Поэтому уже в 1972 году встал вопрос о финансировании модернизации «SkyNet». В результате сегодня орбитальная группировка системы связи состоит их 3-х спутников «SkyNet-4» и 3-х спутников «SkyNet-5».

Уже в конце 1960-х годов ШКПС перешел к компьютерной рассылке части радиоразведывательных сводок заинтересованным получателям в британском правительстве. А в начале 1970-х годов синие папки с данными радиоразведки исчезли из обихода. Их сменил оперативный компьютерный доступ к их электронному хранилищу.

Начиная с 1970-х годов, ШКПС стал внедрять ЭВМ на всех

стадиях своего радиоразведывательного цикла. Однако разрыв между желаемым и действительным был слишком велик. Так, в 1973 году в ШКПС все еще не был завершен процесс компьютерной каталогизации бумажных папок со служебной информацией.

Большую часть парка ЭВМ ШКПС составляло оборудование американской корпорации «IBM». ШКПС приобретал компьютеры «IBM» не только для того, чтобы обеспечить совместимость используемого оборудования с АНБ, но и потому что они воплощали все самые передовые достижения науки и техники того времени.

В ШКПС издавна сложилась практика отбирать самую интересную радиоразведывательную информацию для включения в так называемую «синюю книгу» для Премьер-министра. Маргарит Тэтчер с большим интересом знакомилась с ней, хотя сотрудники ее аппарата с презрением именовали «синие книги» ШКПС комиксами.

А в 1976 году ШКПС закупило в США мощные суперкомпьютеры «Cray-1». Это позволило англо-американским криптоаналитикам возобновить дешифровку и чтение советской шифрпереписки, включая шифрованные сообщения между Москвой и советским посольством в Вашингтоне.

Фолклендская война 1982 года заставила Великобританию обратить самое серьезное внимание на свое отставание от США и Советского Союза в реализации собственных космических программ. Вскоре после ее начала британцам удалось уговорить американцев начать делиться радиоразведывательной информацией со своих спутников.

Чтобы наблюдать за Аргентиной, АНБ на несколько часов в сутки меняло положение своих спутников РЭР, в остальное время направленных на Центральную Америку, где США пристально следили за развитием событий в Никарагуа и Сальвадоре. Однако для британцев это было лишь временное решение давно назревшей проблемы.

Прекрасно понимая, что будущее радиоразведки тесно связано с космосом, в свой последний год пребывания на посту директора ШКПС Брайан Джон Мейнард Тови предложил Тэтчер выделить деньги на разработку и запуск на орбиту собственных спутников радиоразведки.

Хотя бюджет ШКПС составлял более 80% всех финансов, выделяемых правительством Великобритании на спецслужбы, ШКПС их все равно не хватало, чтобы обзавестись спутниковой радиоразведкой.

По некоторым оценкам, на сами спутники радиоразведки,

которые окрестили «Цирконами», а также на связанное с ними наземное оборудование требовалось около 700 миллионов долларов. По истечении 5 лет запущенные «Цирконы» подлежали замене.

В 1983 году директором ШКПС стал Питер Мэричерч и попытался модернизировать британскую радиоразведку, чтобы уйти от старомодных методов проведения радиоразведывательных операций, когда сотрудники тесными рядами сидели в наушниках в неудобных бараках.

Рабочие места операторов станций радиоперехвата были оснащены компьютерными консолями, позволявшими сразу же отправлять заслуживавшие внимания данные радиоразведки в централизованное хранилище. При Меричерче также было введено в эксплуатацию новое звукозаписывающее оборудование и система сравнения перехваченных радиосигналов.

Великобритания нуждалась в таком количестве спутников радиоразведки, которое бы обеспечило контроль всего земного шара. Однако денег у британцев хватало только на один «Циркон», который в конечном итоге и был запущен 4 сентября 1990 года над Азией. Остальную зону покрытия британцам обеспечили американские спутники за 500 миллионов фунтов стерлингов. За эти деньги ШКПС стал «подписчиком» на радиоразведывательную информацию со спутников АНБ, нацеленных на другие регионы.

В 1997 году ШКПС лишился своей старейшей станции перехвата в Гонконге, которая начала функционировать еще во времена «Правительственной школы кода и шифра». Китай получил суверенитет над Гонконгом, и британцы были вынуждены покинуть свою колонию.

В течение многих лет британские дипломаты жаловались, что станция радиоперехвата в Гонконге добывала слишком много разведывательных данных о Китае и задавались вопросом, зачем это делается. А основная причина состояла в повышенном интересе, который проявляли к Китаю американцы.

Гонконг был самым ценным источником радиоперехвата, который АНБ получало от ШКПС, хоть как-то компенсируя дисбаланс в их отношениях. Несмотря на то, что британцы должны были вскоре уйти из Гонконга, американцы продолжали финансировать модернизацию и расширение гонконгской станции радиоперехвата.

В 1982 году на южном берегу острова была сооружена новая станция перехвата спутниковых коммуникаций «Demos-1». На узком каменном уступе, возвышавшемся над водами Южно-Китайского моря, едва хватило места, чтобы установить

5 антенных «тарелок» для контроля сигналов со спутников.

Несмотря на шаткость своего положения, в 1980-е годы станция «Demos-1» продолжала активно модернизироваться. В первую очередь было увеличено количество антенн, чтобы успевать следить за растущим объемом спутниковых коммуникаций Китая. Новые антенны были сконструированы в АНБ по последнему слову науки и техники. Их изготовлением в Калифорнии занималась американская корпорация «Lockheed».

В результате воплощения в жизнь 5-летней программы модернизации «Demos-1» появилось укрепленное инженерное сооружение – станция радиоперехвата «Demos-2». Были выполнены сложные земляные работы и возведены подпорные стены, чтобы она не сползла в море.

Что касается Европы, то ни одна другая страна не подходила так хорошо для США с целью прослушки европейских стран, как Германия. Штаб АНБ, который расположен в форте Джордж Мид в штате Мэрилэнд, именно здесь разместил свою европейскую команду «NCER» (англ. NSA/CSS Europe).

Штаб «NCER» в свою очередь разместился в штабе Командования американских войск в Европе «USEUCOM» (англ. United States European Command) в Штутгарте-Файхингене. Филиалы АНБ размещены также в Аугсбурге, Берлине, Франкфурте, Лангене и Кёльне, равно как и в других европейских странах.

В советский период ни в каком другом месте американская сеть перехвата не была такой густой, как в ФРГ и Западном Берлине. Здесь находилось более 350 центров секретных служб, штабов и отделений различных ведомств США. Американские радиозакладки находились в посольствах и консульствах, на складах оружия и в казармах.

При этом только около 60 из них работали на ЦРУ, а на АНБ – более 600. Сотрудники спецслужб Армии США сидели за магнитофонами и радиоприемниками на горе Тойфельсберг в Западном Берлине, а также в казармах «Шеридан» в Аугсбурге.

Так, в 1951 году на высоком около 100 метров искусственном холме Тойфельсберг в Западном Берлине (Грюневальде) американцы построили станцию радиоразведки, куда завезли технику для прослушки телекоммуникаций ГДР. В 1964 году временные сооружения были заменены на постоянные здания.

В 1967 году в комплексе станции появилось отдельное здание британской армейской радиоразведки «SSD» (англ. Special Signals Division), которое подчинялось ШКПС. Кроме того, там работали отдельные французские специалисты.

Проходя в 1982 году военную службу в Западном Берлине,

сержант Армии США Джеймс Холл вышел на советскую разведку и предложил свои услуги – информацию по базе в Тойфельсберге. Служивший на базе радиошпионажа 23-летний Холл имел допуск к сверхсекретной информации, так как до Берлина успел послужить в Шнееберге, где находился другой центр электронной разведки.

С 1983 года Холл также начал сотрудничать с МГБ ГДР «Штази». После 4-х лет работы восточногерманская разведка решила отметить его заслуги и пригласила в Берлин на встречу с Эрихом Мильке и Маркусом Вольфом, где ему была вручена медаль «За боевые заслуги» МГБ ГДР и 5 тысяч долларов.

За 4 года службы в Тойфельсберге Холл передал «Штази» и КГБ сотни сверхсекретных документов, в том числе информацию по проекту «Троян», – мировой сети электронного наблюдения, которую в военное время можно было использовать для определения местонахождения бронетехники, ракет и самолетов – путем записи радиопередач их раций.

Кроме того, в результате деятельности Холла была выведена из строя компьютерная программа, которая имела целью определение слабых мест в системе советских военных коммуникаций.

В 1984 году он поступил в полное распоряжение «Штази». В апреле 1985 году Холла перевели в 513-ю группу разведки в Форт-Монмут (Нью-Джерси), и он снова вернулся на связь к КГБ.

В феврале 1988 года Холл закончил школу уоррент-офицеров и был направлен в разведотдел 24-й пехотной дивизии, где его связь с КГБ прервалась. К тому времени от КГБ и «Штази» в общей сложности он получил 300 тысяч долларов.

20 декабря 1988 года Холл был взят с поличным американской контрразведкой, сотрудники которой представились сержанту агентами КГБ, решившими восстановить связь. 10 марта 1989 года Холл был приговорен к 40 годам пребывания в военной тюрьме США в Форт-Ливенуорте.

В августе 1990 года станция на горе Тойфельсберг была закрыта, а оборудование вывезено на военную базу в Бад-Айблинге. Там АНБ установило центр управления всеми вращающимися на нижней орбите спутниками-шпионами, перехватывающие из эфира электронные сигналы с территории Германии. Контролируются все факсы, телефонные звонки и письма по электронной почте.

Бункер станции радиоперехвата, уходящий в землю на глубину 6 этажей, куда не имеют доступа немецкие разведчики, является составной частью системы «Эшелон» АНБ. Система направлена в основном не на военные сведения,

а служит целям экономического шпионажа против гражданских предприятий, а также политического шпионажа.

В 1994 году АНБ передало функции управления базой командному центру разведки, одной из центральных спецслужб США. В 2004 году база была возвращена правительству Германии, а станция перемещена в Грисхейм, 7 км к западу от Дармштадта.

Все время американское «ухо» функционировало так эффективно и настолько широкомасштабно, что улавливало и те звуки, которые выходили далеко за рамки потребностей США в области обеспечения собственной безопасности. С территории ФРГ США не только перехватывали сигналы РЛС советских пунктов ПВО.

Антенны и приемные устройства, будь то в Западном Берлине, Браунлаге или Бад-Айблинге, было несложно настроить на любую частоту радиорелейных линий связи, по которым, например, Немецкая федеральная почта передавала в ФРГ почти каждый третий телефонный разговор.

Федеральное ведомство по охране конституции и федеральная уголовная полиция Германии продолжали пользоваться этой мощной системой радиоразведки США, которая, словно громадный пылесос, «высасывала» любую информацию из линий радиосвязи Немецкой федеральной почты.

Кроме того, АНБ использует своих немецких партнёров по электронной разведке для того, чтобы следить за гражданами США. Так, БНД использовала системы, предоставляемые ей АНБ, в том числе «X-Keyscore», чтобы отслеживать определенные «параметры» – номера телефонов, адреса электронной почты, URL-адреса интернет ресурсов, и IP-адреса, чтобы следить за коммуникациями сотрудников в посольстве США в Берлине.

Как ни странно, в посольстве США в Берлине также находится блок АНБ, предназначенный для мониторинга коммуникаций высшего звена немецких правительственных чиновников и высших должностных лиц БНД.

В настоящее время, слежка БНД в значительной степени проводится с бывшей базы АНБ в Бад-Айблинге в Баварии. База находится под контролем БНД и была модернизирована АНБ по договору 2002 года между АНБ и БНД. Небольшой контингент персонала АНБ в настоящее время обеспечивает техническое обслуживание и другую поддержку. Персоналу АНБ в Бад-Айблинге, наверняка, известно об использовании «X-Keyscore» и других систем для шпионажа за дипломатическим, военным, и разведывательным персоналом США при Посольстве США в Берлине.

В 2012 году Разведывательное сообщество Евросоюза ввело

в эксплуатацию крупнейший на территории Западной Европы центр РЭР. Он расположен на глубине 800 метров под горным массивом Сен-Готард, в районе населённого пункта Седрун. Строительство велось одновременно с возведением базового железнодорожного тоннеля Сен-Готард, что позволило сохранить сам факт существования объекта в тайне.

Объект огромен. Он расположен на 4-х уровнях, состоит из 5 блоков. Общая длина тоннелей – более 50 километров. Блоки изолированы друг от друга, соединяет их подземная железная дорога. С поверхностью подземное сооружение соединяется двумя шахтами, в каждой из которых смонтированы четыре грузопассажирских подъёмника.

Действительно, здесь находится самая большая распределённая база данных, хранящая сигнальный трафик и трафик данных практически 90% сетей электросвязи Европы. Сигналы трафика телефонных сетей и Интернета перехватываются наземными станциями радиоперехвата и передаются для анализа по секретным линиям связи.

Высокопроизводительные компьютеры анализируют потоки данных, по ключевым словам выбирают интересные для спецслужб фрагменты датаграмм и передают их для окончательного анализа в аналитическую службу. Аналитики круглосуточно ведут мониторинг открытых данных, формируя «выжимки» – аналитические отчёты.

Практически на каждого жителя Европы тут открыто электронное досье. Компьютеры подбирают в историю жизни, как тут говорят, «лайфлог», всё, что относится к тому или иному гражданину. Медицинские записи и истории болезни, данные о кредитах, правонарушениях, историю переписки в Интернете, телеграммы, телефонные звонки.

Система достаточно легко устанавливает все телефонные номера, которыми пользуется в течение жизни тот или иной объект наблюдения, и по команде оператора начинает сбор информации, которая помещается на электронные носители и хранится практически вечно.

В последнее время тут экспериментируют и с роботизированными системами, которые могут выявлять признаки террористической и экстремистской активности, то есть начинать запись разговоров не по команде оператора, а по данным отобранных запросов. Решение о постановке того или иного гражданина на контроль принимают роботы.

Создание такого центра РЭР является образцом высочайшего уровня военного искусства, с одной стороны, и величайшей демонстрацией цинизма, с другой. Европейские политики

«с пеной у рта» популяризуют Интернет, утверждая, что это «подлинное средство демократии».

Но на деле в создание систем РЭР вкладываются огромные средства. Строительство объекта под горным массивом Сен-Готард обошлось в 9,8 миллиардов швейцарских франков (приблизительно равен доллару). Эти деньги были выделены европейскими правительствами тайно, без всякого общественного обсуждения.

12. Радиолокаторы Чехии

В конце 1950-х годов в Чехословакии был осуществлен главный прорыв в разработках радиолокатора, основной принцип действия которого позже был назван «TDOA» (англ. Time Difference of Arrival – временная разница прибытия). Его суть заключается в измерении 3-мя радиоприемниками, которые находятся на некотором удалении друг от друга, временной разницы излучения, эмитируемого воздушной, наземной или морской целью. На основании этих данных можно «пассивно», т. е. без облучения цели, определить ее местоположение.

Метод «TDOA» изучался и в дальнейшем дорабатывался в чехословацких научно-исследовательских институтах. В 1963 году был создан первый опытный образец для отработки технологии этой идеи, на базе которого появился серийный образец «PRP-1» (чеш. Presny Radiotechnicky Patrac – точный радиотехнический обнаружитель).

Система состояла из 4-х кабин, размещавшихся на полуприцепах, буксируемых среднетоннажными грузовыми автомобилями «Praga». Время развертывания станции «PRP-1» составляло несколько дней. В системе использовались аналоговые комплексы обработки сигналов, волноводы и коаксиальные технологии.

Станция «PRP-1» «Korač» была способна обнаруживать радиолокаторы, работавшие в диапазонах длин волн «L», «S» и «X», бортовые ответчики и ответчики навигационной системы «TACAN». Станция была способна сопровождать от 1-й до 6-и целей. В вооруженных силах ЧССР станция «PRP-1» использовалась до 1979 года.

Второе поколение систем пассивной РТР, которое было действительно, полноценно функционирующим, получило наименование «Ramona». Первоначально система была разработана под шифром «PRP-2» фирмой «Tesla» с 1967 года. В 1980—81 годах она была принята на вооружение и получила новый индекс «KRTP-81» (чеш. Komplet Radiotechnickeho Pruzkumu – комплекс РТР).

Позже была проведена модернизация системы, которая получила обозначение «KRTP-81M» «Ramona-M». Комплекс предназначался для ведения разведки на стратегическом уровне. Станция «Ramona» состояла из 3-х 25-метровых мачт, увенчанных громоздким куполом, прикрывающем антенны, микроволновые части, среднечастотные предусилители и радиорелейные передатчики для обеспечения обмена информацией между

базовой станцией и соседними.

Станция «KRTP-81» способен обнаруживать воздушные, наземные или морские цели, излучающие электромагнитную энергию в диапазоне 0,8…18 ГГц. По сравнению со станцией «PRP-1» новая «Ramona» и ее модификация «Ramona-M» были значительнее эффективны и способны сопровождать в полуавтоматическом режиме до 20 целей в секторе 100° относительно центральной станции комплекса.

Всего в ЧССР было произведено 17 станций «Ramona», 14 станций «Ramona-M» и 1 учебная станция. Из этого количества в СССР было поставлено 14 станций «Ramona» и 10 станций «Ramona-M», 1 станция «Ramona» была продана ГДР, 1 станция «Ramona», 2 станции «Ramona-M» и 1 учебная станция поставлялись в Сирию, и, наконец, 1 станция «Ramona» и 2 станции «Ramona-M» были на вооружении в Чехословакии.

Станции «Ramona», несмотря на свои высокие характеристики, оставались очень сложными в эксплуатации, громоздкими и требовалось от 4 до 12 часов на их развертывание. Одна система размещалась на 13 тяжелых грузовых автомобилях «Tatra». В классификации НАТО станции «Ramona» и «Ramona-M» получили обозначение «Soft Ball».

После многих лет разработки и эксплуатации станций первых поколений «PRP-1» и «KRTP-81» появилось понимание, что заказчику необходима реально мобильная система с гораздо высокими характеристиками по обнаружению целей. Плюс к этому моменту появилась новая элементная база. Это все позволило начать реализацию в 1981—83 годах нового проекта, которому дали женское имя «Tamara».

В отличие от советского географического принципа именования собственных систем ПВО, страны Варшавского договора, особенно Польша и Чехословакия, использовали в качестве обозначений РЛС женские имена. Новая система РТР «Tamara» поступила на испытания в конце 1983 года.

Всего было предусмотрено 3 варианта этой системы. Испытания мобильной разведывательной станции проходили с сентября 1984 года до конца 1985 года. Войсковые испытания станции под обозначением «KRTP-86» были проведены летом 1987 года, а 10 октября 1987 года прошли государственные испытания системы.

Станция «Tamara» может использоваться как для ведения стратегической, так и тактической разведки. «Tamara» способна обнаруживать радиолокаторы, излучатели радиолокаторов, передатчики системы «свой-чужой», навигационные системы «TACAN», дальномеры системы «DME», системы обмена

тактической информацией «JTIDS», а также постановщики активных помех, работающие в диапазоне 0,82…18 ГГц.

Во время испытаний новая система обнаруживала цель типа «F-16» на дальности 400 км, «CF-18A» – 355 км, «F-15» – 365 км. Более старые истребители типа «F-4» засекались на отметке 395 км, «F-104» – 425 км.

Станция пассивной РТР «Tamara» в начале 1989 года была принята на вооружение чехословацкой армии. Основным вариантом системы был автомобильный. Самоходная станция «Tamara» состоит из 8 единиц техники, размещенных на автомобильном шасси «Tatra».

В ее составе 3 приемных устройства «RS-AJ/M», 1 аппаратная кабина приемного комплекса «RS-KB», аппаратная кабина обработки сигналов «RS-KM», а также дополнительно может быть развернут командный модуль «ZZP-5» с системами отображения информации.

Приемное устройство «RS-AJ/M» представляет собой антенну цилиндрической формы, установленную на телескопическом подъемном устройстве, которое смонтировано на автомобильном шасси «Tatra» с колесной формулой 8х8.

Шасси было доработано путем установки 4-х гидравлических домкратов для горизонтирования антенно-мачтового устройства (далее – АМУ), а перед водительской кабиной был навешен бульдозерный нож для подготовки боевой позиции.

АМУ может подниматься на высоту 8,5 метров или в промежутке от 12,5 до 25 метров. В цилиндрической форме обтекателя АМУ находятся необходимые антенны и приемники, микроволновые передатчики для обмена информацией между компонентами комплекса.

Поднятая антенна способна противостоять ветру со скоростью не более 50 м/с, а работа станции возможна при силе ветра не более 30 м/с. На боевой позиции приемные устройства «RS-AJ/M» размещаются на удалении друг от друга от 10 до 35 км.

Стационарный вариант «Tamara» состоит из 3-х антенных модулей, установленных в специальных контейнерах с габаритами 3,5х3,5х3 м на 25-метровых мачтах. В период 1994—95 годов эта версия комплекса предлагалась на международных выставках чешской компанией «HTT-Tesla Pardubice» под обозначением «Flora».

Дальность обнаружения станцией РТР «Tamara» составляет 450 км и ограничена только радиогоризонтом. Система способна практически в режиме реального времени сопровождать до 72 целей в секторе 100°. «Tamara» находится в серийном

производстве и постоянно модернизируется путем включения в ее состав новых подсистем и алгоритмов обработки информации.

Обновленный комплекс получил обозначение «KRTP-91», его сектор обзора увеличился до 120°. Находящаяся в городе Пардубице компания «Tesla» построила 23 комплекса РТР «Tamara», из которых в СССР было поставлено 15 комплексов, в ГДР – 1 комплекс, а Чехословакия приняла на вооружении 4 комплекса.

В 1991 году США удалось заполучить 1 комплекс «KRTP-91», приобретя ее через Оман. Самоходные версии «Tamara» получили обозначение в классификации НАТО «Trash Bin». Один из комплексов «KRTP-86», приобретенный Советским Союзом, в ноябре 2005 года был обнаружен на склоне горы Ахун неподалеку от Сочи.

После раздела Чехословакии на два государства (Чехия и Словакия) разработка средств РТР продолжилась в Чехии. Благодаря опыту, накопленному при создании комплексов «Kopač», «Ramona» и «Tamara», появилось новое поколение средств пассивной радиолокации, которому присвоили очередное женское имя «Věra».

В 1999 году начались испытания военной системы 4-го поколения «Věra», которая использует сразу 4 приемника. Благодаря этому она может отслеживать положение сотен перемещающихся целей в режиме реального времени. Модель «Věra-S/M» была поставлена на вооружение чешской армии.

Разработку нового комплекса вела компания «ERA» (правоприемник компании «HTT-Tesla» с 1994 года), которая после его готовности начала предлагать для экспортных поставок под обозначением «Věra-E». Ее назначение не отличалось от предшественниц. Тем не менее, современные технологии и новая элементная база позволили сократить размеры и вес отдельных элементов, которые повысили мобильность системы.

Пассивные комплексы относятся к передовым технологиям, нуждающимся в высококвалифицированном персонале, подготовка которого занимает не месяцы, а годы. Система «Věra» также не может эффективно работать без базы характеристик целей, так как полученные сигналы нужно с чем-то сравнивать. Но, несмотря на эти препятствия, на современном поле боя эта система может стать высокоэффективным инструментом.

Диапазон частот, в котором станция может обнаруживать излучение воздушных и наземных целей, составляет 1…18 ГГц и может быть дополнительно расширен до диапазона от 0,1… 1 ГГц до 18…40 ГГц. Станция «Věra-E» может обнаруживать излучение вторичных транспондеров бортовых РЛС

и передатчиков системы госопознавания (1030…1090 МГц), навигационных систем «TACAN» и дальномеров DME (1025…1150 МГц). Сектор обзора «Věra-E» увеличился до 120°, а по желанию заказчика он может быть круговым.

Максимальная дальность обнаружения цели составляет 450 км. Одновременной система «Věra-E» может сопровождать до 200 целей. Темп обновления информации от 1 до 5 сек. Антенный модуль представляет собой цилиндр высотой 2 м, диаметром 0,9 м и весит 300 кг. Двусторонняя микроволновая радиолиния связывает антенный модуль с аппаратным модулем. Кроме того, компания «ERA» продвигает другие версии этой системы, включая гражданские комплексы «Věra-P3D» и «Věra-ASCS».

В январе 2004 года чешская компания по экспорту вооружений «Omnipol» получила от Министерства промышленности и торговли Чехии 2 экспортные лицензии на поставку в Китай 6 комплексов «Věra-E» на общую сумму 58 миллионов долларов. Как только стало известно о 1-м китайском контракте на сумму 23 миллионов долларов, правительство США незамедлительно выразило протест Чехии.

В чешской печати широко освещалось предполагаемое письмо госсекретаря США Колин Пауэлла своему чешскому коллеге Кирилу Свободе касательно продажи Китаю станций «Věra-E», а также личное обращение Колина Пауэлла чешскому премьер-министру Владимиру Спидле, в котором американский госсекретарь просил отменить контракт с Китаем.

В конечном счете после подобного «демократического давления» 19 мая 2004 года чешское правительство аннулировало лицензии на экспорт в Китай комплексов «Věra-E», о чем чуть позже уведомило компанию «Omnipol». Это «высокий» показатель независимости и суверенности государства, входящего в состав Евросоюза и НАТО!

Утверждение о том, что такие комплексы, как «Tamara» и «Věra», способны обнаружить американские «невидимые» самолеты, не совсем точно, но факт в том, что при определенных условиях они могут следить за целями, которые традиционные радары не регистрируют. Так что, возможно, США хотели «подстраховать» безопасность этой технологии.

В настоящее время в Чехии имеется всего лишь 1 станция РТР «Věra-E». В ноябре 2004 года закончилась ее сборка, а уже в декабре 2005 года она была принята на вооружение чешской армии. Станция «Věra-E» базировалась в 53-м Центре РТР и РЭБ в г. Плана, что находится неподалеку от г. Ческе-Будеёвице.

Отговорив Чехию продавать станцию «Vera-E» Китаю, США

сами приобрели в начале 2005 года один комплект «Vera-E» для собственных нужд. Как показывает практика, американцы покупают в единичных экземплярах военную технику только для ее изучения и поиска путей противодействия ее возможностям. Стоимость контракта, включая сервисное обслуживание и обучение персонала, составила 10 миллионов долларов.

Летом 2005 года Чехия продала за 4 миллиона долларов еще одну станцию «Věra-E» Эстонии. В этот период появились сообщения, что Китай не оставляет попыток приобрести комплексы «Věra-E».

Согласно информации пражского еженедельника «Евро», китайская сторона в ходе визита в Пекин чешского премьер-министра Иржи Пароубка вновь поднимала вопрос о закупке «Věra-E», причем решение этого вопроса связывали с предоставлением выгодных условий чешским контрактам в Китае. Кроме Китая, повышенный интерес к «Věra-E» проявляют также Малайзия, Египет, Пакистан и Вьетнам.

В октябре 2006 года фирму «ERA» приобрела американская компания «Rannoch» за 6,25 миллионов евро и перевезла большую часть производства в Пардубице. Однако новый собственник не стремился инвестировать в разработки, которые в этой стремительно развивающейся сфере имеют огромное значение.

Любой, кто хочет добиться в ней успеха, должен постоянно реагировать на то, что может противопоставить потенциальный противник. Но новый владелец был заинтересован в получении быстрой прибыли, а не в долгосрочной стратегии.

«Звезда» компании «ERA» начала «меркнуть», хотя виной тому был не только американский владелец, но и чешские политики. Они, как обычно (за некоторым исключением), делали очень мало для того, чтобы поддержать экспортные достижения пассивных радиолокационных систем своей страны.

В феврале 2007 года «Rannoch» была переименована в «ERA Corporation». В июле 2008 года корпорация была куплена американской ИТ-компанией «SRA International» за 125,5 миллиона долларов. Интересно, что компания предоставляет ИТ-услуги в области национальной безопасности для Министерства обороны, национальной безопасности, армии, ВВС и спецслужб США.

В 2011 году американские владельцы выставили корпорацию «ERA» на продажу как «неперспективную», и новым владельцем стала чешская компания «Omnipol». Несмотря на то, что из-за некоторых заказов для чешской армии (в частности проблемных самолетов «CASA») эта фирма имеет очень противоречивую репутацию, для пардубицкой компании покупка стала, быть

может, спасением в последнюю минуту.

Ведь фирма «Omnipol» была готова выделять средства на развитие, а также делала ставку на то, что в некоторых странах третьего мира бренд «ERA» по-прежнему хорошо известен. Так, при оказанной поддержке на рынке появилась пассивная радиолокационная система 5-го поколения «Věra-NG».

В 2013 году компания «ERA» подписала контракт на поставку 2-х мобильных систем «Věra-NG», а также их материально-техническое обеспечение и обучение операторов. В том же году РЛС была включена в список разрешенной комплектации чешской армии, что открыло возможности ее использования также остальными государствами-членами НАТО.

Контракт был подписан по результатам международного тендера, в котором приняли участие претенденты из 28 стран НАТО. В ходе оценки предложений компания «ERA» провела демонстрацию системы «Věra-NG» в условиях, приближенных к боевым. Компания продемонстрировала возможность системы не только обнаруживать самолеты военной авиации, но и точно их идентифицировать.

Стоимость контракта составила 434 миллиона чешских крон (16 миллионов евро). Контракт профинансирован за счет средств программы НАТО по инвестициям в обеспечение безопасности «NSIP» (англ. NATO Security Investment Programme). Работы должны быть завершены летом 2018 года. Закупленные системы станут частью более широкой системы ПВО и будут размещены на базе НАТО в Северной Италии.

Комплекс предназначен для обнаружения самолетов, автомашин и других объектов, основываясь на технологии пассивного сопровождения источников излучения, включая РЛС, постановщики помех, передатчики системы «свой-чужой», навигационные системы «TACAN», дальномеры системы «DME», средства связи, навигации и системы наблюдения.

Комплекс «Věra-NG» способен обнаруживать, идентифицировать, определять координаты и одновременно сопровождать в секторе 360˚ до 200 воздушных, наземных и морских целей на дальностях до 200 миль (322 км) с точностью до 20 метров. Темп обновления информации – от 1 до 5 сек. На текущий момент «ERA» поставила более 100 систем своего производства гражданским и военным заказчикам более 60 стран.

Эпилог

Чтобы поиграть дома в шпиона или радиоразведчика, надо купить радиоприемник определенного волнового или частотного диапазона. Как известно, радиоволны условно делятся на 4 группы:

– длинные волны (ДВ) – частота 150…450 кГц;

– средние волны (СВ) – 500…1600 кГц;

– короткие волны (КВ) – 3000…30 000 кГц;

– ультракороткие волны (УКВ) – 30…30 000 МГц.

Для «шпионских» радиопосланий наиболее удобны короткие волны. Во-первых, весь диапазон КВ можно легко «прослушать» на обычном КВ или всеволновом радиоприемнике. Во-вторых, КВ распространяются на очень большие расстояния при малой мощности передатчика.

Происходит это потому, что они полностью отражаются от верхних, электрически заряженных слоев атмосферы Земли – ионосферы. И сигнал как бы скачет «вверх – вниз» и обходит всю планету. В отличие от них УКВ «прошивают» ионосферу насквозь и уходят в космическое пространство, а ДВ и СВ – с разной степенью поглощаются ионосферой.

Любители КВ радиопередач нередко натыкаются на загадочные станции, передающие бесконечные последовательности цифр. Поэтому их называют «числовыми», или «номерными», радиостанциями. Непонятный код монотонно зачитывают на разных языках мужские, женские, а иногда и детские голоса.

Странные передачи впервые появились в радиоэфире с середины прошлого века. Сигнал у подобных станций весьма сильный, но они никогда не сообщают ни о месте своего расположения, ни об аудитории, для которой предназначена трансляция. Обычно слушатели, наткнувшись на такую передачу, какое-то время еще пытаются разобрать нескончаемое «три-пять-два-девять…», а потом, сбитые с толку, крутят ручку настройки дальше.

Крайне редко такие радиостанции передают отдельные фразы или тексты. Например, в конце мая 1990 года на частотах, которые по мнению радиолюбителей использовали сотрудники МГБ ГДР «Штази», нестройный хор мужских голосов несколько дней исполнял «Песню про утенка». Она транслировалась на тех же частотах, что и обычные указания «бойцам невидимого фронта».

Вокальные способности офицеров одной из самых

эффективных спецслужб периода «холодной войны» смогли оценить по достоинству только многочисленные «нелегалы» и агенты из ГДР во всем мире: для них передача означала конец карьеры. Между тем, песенку слышали не только разведчики и контрразведчики, но и многочисленные радиолюбители, которые, по всей вероятности, не понимали скрытого в ней смысла, зато педантично фиксировали время каждого сеанса и частоты «шпионских станций».

Примерно с середины 1970-х годов, с появлением новых приемников с цифровыми устройствами для отслеживания передатчиков, радиолюбители-коротковолновики занялись «числовыми станциями» всерьез. К тому времени было уже ясно, что загадочные радиоточки принадлежат шпионским центрам и передают зашифрованные послания для своих агентов в других странах. Радиолюбители составили не только обширные перечни таких станций с точным расписанием их работы, но и занялись радиопеленгацией для установки мест их базирования.

Как известно, радиосвязь в диапазоне КВ обеспечивает трансляцию сообщений на максимально далекие расстояния, связывая между собой даже диаметрально противоположные точки земного шара. Соответственно КВ-радиопередачи представляют собой идеальный инструмент для анонимной односторонней связи. Агент разведки в любой точке планеты может получать послания от руководства с помощью маленького, общедоступного и никак не модифицированного радиоприемника.

Радиолюбители-перехватчики всего мира начали объединяться, поскольку стали активно общаться между собой. В 1980-е годы появился международный клуб радиолюбителей «Привидения» (англ. Spooks), который предпочитает не афишировать себя. По своим техническим возможностям и эффективности работы «привидения» смело могут соперничать со службами радиоразведки ведущих мировых держав.

В середине 1990-х годов часть «привидений» увлеклась радиоразведкой. Их интересовали не только местоположение и параметры (расписание передач, позывные, частоты) отдельных радиостанций, в первую очередь военного назначения, но и содержание сообщений.

В отличие от СССР и впоследствии России, в США даже выпускают справочники с указанием частот наземных служб аэропортов, полиции, армии. В результате за долгие годы мониторинга эфира у членов клуба скопилась информация о том, как в какой период работал обнаруженный передатчик.

То есть фактически каждый сам для себя занимался тем, что

на языке радиотехнической разведки называется «составление графика активности». А это полноценная часть работы разведки, которая позволяет при условии анализа многих данных прогнозировать события.

Но «привидения» – не единственная организация подобного рода. В январе 1995 года начал действовать клуб «WUN» (англ. Worldwide UTE News). Аббревиатура «UTE» означает, что членов клуба интересуют радиостанции, работающие в частотном диапазоне до 30 Мгц. Штаб «WUN» составляют 11 человек из США, Европы, Японии, Новой Зеландии, а простых участников насчитывается уже много больше сотни.

На сегодняшний день почти не осталось мест на планете, которые не попали бы в их поле зрения. Они обменивались друг с другом информацией через интернет. Выпускали и ежемесячный печатный бюллетень, в котором публиковали расписания вещания «числовых станций», то есть их частоты и периодичность выхода в эфир. Сообщали и забавные позывные некоторых станций.

Подобные организации – структура, о которой может только мечтать любая радиоразведка. Во-первых, они неуловимы: в качестве средства общения используют только электронную почту, работают обычно под псевдонимом, никогда сами не выходят в эфир, применяя только аппаратуру для радиомониторинга, благо во многих странах не требуется ее регистрация. В тех случаях, если регистрация официально нужна, как в России, необходимое оборудование всегда можно приобрести на «черном рынке».

Во-вторых, «привидения» и им подобные работают против других стран и тем самым не вступают в конфликт с местными правоохранительными органами. Например, американцы предпочитают слушать передатчики, находящиеся на Кубе, граждане Китая выбирают радиостанции США, а россияне – китайцев. Это связано не только с чувством патриотизма или инстинктом самосохранения, но и с техническими особенностями организации тайной радиосвязи.

В-третьих, для «призраков» характерен высокий уровень оперативности и достоверности. Благодаря «всемирной паутине» любая свежая информация почти мгновенно становится известна всем членам клуба. В-четвертых, радиолюбители исключительно профессиональны и внимательно изучают всю доступную информацию по организации радиоразведки и радиоэлектронной борьбы.

Радиолюбители фанатично ищут любые секретные радиостанции, начиная с армий всех стран мира и заканчивая

авиакосмическими агентствами. Понятно, что в списке есть и радиостанции агентов и нелегальных сотрудников разведок, будь то израильская, американская или российская. Множество радиолюбителей занимаются не только прослушкой и записью передач «числовых станций», но и обычной радиоразведкой.

Если в первом случае ущерб от их деятельности минимальный (технические подразделения контрразведки сами внимательно отслеживают все сеансы связи), то во втором они порой оказываются эффективнее военных. Ведь любители выполняют те же задачи, которые решает радиоразведка, но при этом у них есть уникальная возможность сравнивать данные, которые получены у не зависимых друг от друга операторов, чего не могут позволить себе военные.

Так, например, радиолюбители определили некий передатчик, предположительно, расположенный на Кипре, на базе британских ВВС. У этой станции позывной состоял из нескольких тактов старой английской песенки «Линкольнширский браконьер». Сначала шла музыка, потом длинный звуковой сигнал, и механический женский голос начинал произносить цифры.

В эфире станция присутствовала почти круглосуточно, и поймать с территории России ее было довольно просто. Наиболее вероятно было ее поймать на частоте 11545 кГц, а вообще станция работала во всем КВ диапазоне. Станция передавала за сутки довольно много сообщений. Выходило, что и агентов было много.

А на обычный КВ-приемник, обладая неким опытом, можно поймать сигнал с Кипра почти в любой точке планеты. Впрочем, многое зависит от мощности передатчика и от направления вещания. Похоже, «Линкольнширский браконьер» все же давал указания агентам в Европе, в том числе в России, а также на Ближнем Востоке, в Китае.

Конечно, по радио вы не услышите такое сообщение: «Внимание, внимание! У микрофона в студии израильская разведывательная служба „Моссад“. Не отходите от приемников… После небольшой рекламы мы продолжим передачу сообщения для нашего секретного сотрудника в России».

Тем не менее, спецслужбы активно пользуются радиоэфиром для передачи сообщений своим нелегальным сотрудникам. Тот же «Моссад» (по слухам, разумеется, ведь никто напрямую не признается) вещает ежедневно на частотах 4780, 4880 и 9130 кГц. И прослушать шпионские передачи может любой человек, имеющий КВ радиоприемник.

Прослушать вы можете, но понять нет, поскольку все

сообщения закодированы. В эфире диктор попросту перечисляет ряды 5-значных чисел. В «радиожизни» спецслужб со времен легендарного разведчика Отто фон Штирлица изменилось только одно – шпионских передач стало гораздо больше.

Много передач идет на английском языке. Впрочем, слушать их могут не только англичане и американцы. Передаются сообщения и на немецком, испанском, славянских языках. Русскоязычных посланий тоже много. Впрочем, определить принадлежность станции можно только на уровне догадок.

Согласно данным мониторинга радиоэфира 30 марта 2017 года на частоте 14212 кГц работала «номерная» радиостанция, передавая шифрованные сообщения женским голосом на русском языке. В релизе сообщается, что работала станция СВР Украины в Ровно. Ранее о работе подобных радиостанций сообщалось в начале 2017 года, но тогда работа велась на частоте 7060…7070 кГц.

В связи с широким развитием интернета такой способ односторонней агентурной радиосвязи может и покажется уже архаизмом, но свое значение он сохраняет: принимающего такие радиопередачи принципиально невозможно обнаружить, если только не застать его лично в момент сеанса. Сеансы же связи через компьютерные сети теоретически могут быть отслежены до компьютера агента.

И что интересно, во время августовского путча 1991 года, осады и штурма «Белого дома» в 1993 году, после знаменитой речи Бориса Ельцина об отставке 31 декабря 1999 года, перед выборами Президента РФ и депутатов в Госдуму интенсивность шпионских радиопередач на русском языке росла. Очевидно, какие-то спецслужбы хотели повлиять на эти процессы, используя свои шпионские сети…

Использованная литература

1. Анин Б., Петрович А. Радиошпионаж. «Международные отношения», 1996.

2. Батюшин Н. Тайная военная разведка и борьба с ней. София, 1939.

3. Бухгайт Г. Абвер – «щит и меч» III Рейха. М., 2013.

4. Вагнер А., Уль М. БНД против Советской армии: Западногерманский военный шпионаж в ГДР. Киев, 2008.

5. Ваннах М. Разведка ФРГ открывает охоту на соцсети // http://www.computerra.ru/100431/razvedka-frg-otkryivaet-ohotu-na-sotsseti/ – 2014.

6. Визингр Л. Чешские системы разведки набирают очки // http://inosmi.ru/military/20160707/237099005.html – 2016.

Гольев Ю., Ларин Д., Тришин А., Шанкин Г. Служба наблюдения Кригсмарине. «Защита информации. INSIDE» №5, №6. 2006.

7. Иванов И., Чадов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века. Зарубежное военное обозрение №1, 2011.

8. Клепов А. Информационное оружие Гитлера // www.proza.ru/ 2009/06/17/949.

9. Колесов П. Стрелецкий А. Разведывательные службы ВС Франции. «Зарубежное военное обозрение», №3, 2007.

10. Кустов П. Шпионы – радиолюбители. Незримы и очень опасны // www.qrz.ru/articles/article195.html – 2003.

Лазаревич А. Сен-Готард: шпионы из преисподней // http:// forum-msk.org/material/fpolitic/9670296.html – 2013

11. Маклахлан Д. Тайны английской разведки (1939—1945). М., 1971.

12. Малеванный В. Глобальный электронный перехват. «Независимое военное обозрение», 11.08.2000.

13. Печуров С. Шпионаж и контршпионаж по-джентльменски // http://nvo.ng.ru/spforces/2015-04-24/8_england.html – 2015.

14. Писарев В. Службы разведки и безопасности Великобритании. «Зарубежное военное обозрение» №4/2000.

15. Райле О. Тайная война. Секретные операции абвера на Западе и Востоке (1921—1945). М., 2002.

16. Ронге М. Разведка и контрразведка (1939). М., 2004.

17. РЭБ в современной войне // www.modernarmy.ru/ article/163 – 2012.

18. Стефанович А. История успехов и неудач шведской радиоразведки (1914—44). «Защита информации. Конфидент»

№2, 2001.

19. Ульфкотте У. Совершенно секретно: БНД. За кулисами Федеральной разведывательной службы Германии. М., 2005.

20. Хайнц Х. Пароль – Директор. М., 2003.

21. Хиршманн К. Секретные службы. Гамбург, 2004.

22. Хьюз-Уилсон Д. История катастрофических провалов военной разведки. Екатеринбург, 2014.

23. Чехословацкие станции пассивной электронной разведки // http://pvo.guns.ru/other/czech/tamara/ – 2008.

Использованные веб-сайты

Великие операции спецслужб // http://greatoperation.narod.ru

Проект «Агентура» // www.agentura.ru

Свободная энциклопедия «ВикипедиЯ» // http:// ru.wikipedia.org

Рекомендованные фильмы

Документальные

Секретная война: Всё ещё тайна (Великобритания, 1977)

Тайны века: Зашифрованная война (Россия, 2003)

Шпионы и предатели: берлинский туннель (Россия, 2008)

Тайная война: Радиоперехват (Россия, 2010)

Забытые герои Блетчли Парка (Великобритания, 2011)

Шпионы в берлинском тоннеле (США, 2011)

Две жизни Джорджа Блейка, или агент КГБ на службе Её Величества (Россия, 2012)

Вам и не снилось. Цифровой апокалипсис (Россия, 2014)

Художественные

Энигма (Великобритания, Германия, США, 2001)

Поединки: выбор агента Блейка (Россия, 2011)

Игра в иммитацию (Великобритания, США, 2014)

Об авторе

Гребенников Вадим Викторович родился 20 апреля 1960 года в Ужгороде, столице Закарпатья, которое до 1945 года называлось Подкарпатской Русью, а поэтически – Серебряной Землёй.

Имеет высшее техническое образование: закончил в 1982 году Ленинградский электротехнический институт связи имени профессора М. А. Бонч-Бруевича (ЛЭИС, ныне – СПбГУТ – Санкт-Петербургский Государственный университет телекоммуникаций) по специальности «радиотехника» и получил квалификацию радиоинженера с присвоением первичного воинского звания «лейтенант».

Женился в ноябре 1984 года, имеет 3-х детей, 2-х внучек и внука. Полковник, ветеран и пенсионер. Живёт в Ужгороде.

В феврале 1983-го начал работать на должности

электромеханика в отделении правительственной связи (далее – ПС) Управления КГБ УССР по Закарпатской области, а в 1986-м стал офицером и начал прохождение военной службы в том же подразделении на должности инженера отделения ПС. В 1987-м был переведён на должность инженера группы ПС Мукачевского горотдела УКГБ.

В марте 1992 года на базе КГБ УССР в Украине была создана Служба безопасности (далее – СБУ), и с 1993 года продолжил службу начальником отделения ПС Мукачевского горотдела Управления СБУ в Закарпатской области. Ужгородское отделение ПС было реорганизовано в Отдел ПС Управления СБУ в Закарпатской области.

Летом 1998 года Главное Управление ПС СБУ и Главное управление ТЗИ Госкомсекретов Украины были реорганизованы в Департамент специальных телекоммуникационных систем и защиты информации (далее – ДСТСЗИ) СБУ, в структуру которого ввели Отдел ПС областных управлений СБУ. В декабре того же года был организован Отдел ДСТСЗИ СБУ в Закарпатской области (далее – Отдел).

В 2000 году автор был переведён из Мукачева в Ужгород на должность начальника оперативно-технического управления Отдела. В 2002 году был назначен начальником отделения правительственной и конфиденциальной связи Отдела, а в 2003 году – помощником начальника Отдела по вопросам безопасности связи.

В начале 2006 года Верховным Советом Украины был принят Закон «О Государственной службе спецсвязи и защиты информации Украины», введённый в действие с 1 января 2007 года. В соответствии с этим законом ДСТСЗИ был выведен из состава СБУ и на его базе создана самостоятельная Госслужба спецсвязи и защиты информации Украины (далее – Госспецсвязи), а также её региональные органы.

1 января 2007 года автор был назначен на должность заместителя начальника Управления Госспецсвязи в Закарпатской области. 29 сентября того же года принял участие в аварийном восстановлении и обеспечении безопасности функционирования информационно-аналитической системы «Выборы», за что 13 ноября 2007 года Указом Президента Украины №1092 был удостоен медали «За безупречную службу».

После увольнения со службы в 2012 году автор издал на украинском языке книгу «История криптологии & секретной связи» (800 страниц), которую писал на протяжении 15 лет и фактически стал историком криптологии, стеганографии и специальных видов связи.

После этого разработал официальный WEB-сайт книги, который постепенно с увеличением выложенных на нём материалов превратился в историчесий портал по информационной безопасности (далее – ИБ). Сейчас он содержит не только русскую версию книги, исторические статьи, фильмы и фотографии, но и учебные материалы для студентов Ужгородского национального университета (далее – УжНУ) по ИБ и защите информации.

В 2017 году была переиздана первая часть написанной книги под названием «Криптология и секретная связь. Сделано в СССР» (480 страниц) московским издательством «Алгоритм» (ISBN 978-5-906979-79-7). В ней излагается история криптологии и специальных видов связи в Российской империи и Советском Союзе.

Автор работает старшим преподавателем по ИБ в УжНУ, где читает лекции по следующим учебным дисциплинам: «Нормативно-правовое обеспечение ИБ», «Управление (менеджмент) ИБ» и «Комплексные системы защиты информации: проектирование, внедрение, сопровождение».

С монографией, фильмами и другими материалами по истории стеганографии, криптологии и специальных видов связи, а также по информационной безопасности и защите информации можно ознакомиться по адресу: **http://cryptohistory.ru**

Примечания1

Террористическая организация, запрещенная в РФ